A compliance guide for practitioners

MASTERING ANTI-MONEY LAUNDERING AND COUNTER-TERRORIST FINANCING

- Build an effective compliance framework for your business
- Contains draft forms, checklists and risk-assessment tools
- Rich with case studies and examples
- Fully revised and updated

SECOND EDITION

TIM PARKMAN

FT PUBLISHING
FINANCIAL TIMES

Mastering Anti-Money Laundering and Counter-Terrorist Financing

A compliance guide for practitioners

TIM PARKMAN

Second edition

Harlow, England • London • New York • Boston • San Francisco • Toronto • Sydney • Dubai • Singapore • Hong Kong
Tokyo • Seoul • Taipei • New Delhi • Cape Town • São Paulo • Mexico City • Madrid • Amsterdam • Munich • Paris • Milan

At Pearson, we have a simple mission: to help people make more of their lives through learning.

We combine innovative learning technology with trusted content and educational expertise to provide engaging and effective learning experiences that serve people wherever and whenever they are learning.

From classroom to boardroom, our curriculum materials, digital learning tools and testing programmes help to educate millions of people worldwide – more than any other private enterprise.

Every day our work helps learning flourish, and wherever learning flourishes, so do people.

To learn more, please visit us at **www.pearson.com/uk**

Mastering Anti-Money Laundering and Counter-Terrorist Financing

PEARSON EDUCATION LIMITED

KAO Two
KAO Park
Harlow CM17 9SR
United Kingdom
Tel: +44 (0)1279 623623
Web: www.pearson.com/uk

First published 2012 (print and electronic)
Second edition published 2019 (print and electronic)

© Pearson Education Limited 2012, 2019 (print and electronic)

The right of Tim Parkman to be identified as author of this work has been asserted by him in accordance with the Copyright, Designs and Patents Act 1988.

The print publication is protected by copyright. Prior to any prohibited reproduction, storage in a retrieval system, distribution or transmission in any form or by any means, electronic, mechanical, recording or otherwise, permission should be obtained from the publisher or, where applicable, a licence permitting restricted copying in the United Kingdom should be obtained from the Copyright Licensing Agency Ltd, Barnard's Inn, 86 Fetter Lane, London EC4A 1EN.

The ePublication is protected by copyright and must not be copied, reproduced, transferred, distributed, leased, licensed or publicly performed or used in any way except as specifically permitted in writing by the publishers, as allowed under the terms and conditions under which it was purchased, or as strictly permitted by applicable copyright law. Any unauthorised distribution or use of this text may be a direct infringement of the author's and the publisher's rights and those responsible may be liable in law accordingly.

All trademarks used herein are the property of their respective owners. The use of any trademark in this text does not vest in the author or publisher any trademark ownership rights in such trademarks, nor does the use of such trademarks imply any affiliation with or endorsement of this book by such owners.

Pearson Education is not responsible for the content of third-party internet sites.

The Financial Times. With a worldwide network of highly respected journalists, *The Financial Times* provides global business news, insightful opinion and expert analysis of business, finance and politics. With over 500 journalists reporting from 50 countries worldwide, our in-depth coverage of international news is objectively reported and analysed from an independent, global perspective. To find out more, visit www.ft.com/pearsonoffer.

ISBN: 978-1-292-28235-0 (print)
978-1-292-28236-7 (PDF)
978-1-292-28237-4 (ePub)

British Library Cataloguing-in-Publication Data
A catalogue record for the print edition is available from the British Library

Library of Congress Cataloging-in-Publication Data
A catalog record for the print edition is available from the Library of Congress

10 9 8 7 6 5 4 3 2 1
23 22 21 20 19

Print edition typeset in 11.5pt Garamond 3 LT Std by SPi Global
Print edition printed and bound in Malaysia

NOTE THAT ANY PAGE CROSS REFERENCES REFER TO THE PRINT EDITION

Contents

Acknowledgements
Disclaimer
Introduction
About the author

1 Fundamental Concepts

Background and definitions
Key processes in money laundering and terrorist financing
Money laundering
Crypto-Laundering and the Blockchain
Terrorist financing
Further differences between terrorist financing and classical money laundering
Suspicion recognition

2 The International AML and CFT Framework

Key components of the international institutional and legal framework
A developing framework to combat tax evasion
Proliferation Financing

A developing framework for the regulation of cryptocurrencies

The Financial Action Task Force (FATF)

FATF regional style bodies and associate members

Other relevant international bodies

Key requirements for financial institutions

Key components of a national AML/CFT framework

3 The Role, Structure and Positioning of the AML/CFT Compliance Function

Structure and culture

AML/CFT best practice

Best practice in higher-risk products and services

IT systems

The use of artificial intelligence

Training, communication and awareness

A ‘pro-business’ approach

Management of internal suspicion reporting

4 CDD, KYC and the Risk-based Approach

Background to the Risk-Based Approach

Components of the Risk-Based Approach

Mitigating controls

Regulatory environment

Special categories: Politically Exposed Persons (PEPs)

Constructing a Risk-Based Approach for your organisation

The core components of CDD

CDD processes and tools

Example risk assessment frameworks

Constructing a CDD framework for financial institutions

Constructing a CDD framework for retail/consumer banking business

Constructing a CDD framework for private banking

5 Reputational Risk

Managing reputational risk

When banks go wrong: cases of punishments and penalties

Managing reputational risk: the experience of the MDBs

The integrity ‘red flags’ checklist and the due diligence investigation tools

Practical application

6 Suspicion Recognition

Background and general principles

Money laundering typologies

Terrorist financing typologies

Account analysis examples

‘Accumulation of evidence’ cases

The 21st century: areas of rising concern

7 International Cooperation

Background

Modern structures of organised crime and terrorism

Mechanisms and tools of international cooperation

International cooperative bodies

8 Modern Money Laundering and Terrorist Financing: Two Case Studies

Introduction

Smoke and Mirrors: AlnaBank and the Messengers of God

Futura Capital Partners: Modern Money Laundering through 'low risk' regulated OECD Financial Institutions

Discussion Points: Futura Capital Partners Case

Appendix

Index

Author's acknowledgements

The author wishes to thank Gill Peeling and Stuart Hammond for their hard work in assisting with the preparation of this book, along with numerous industry colleagues and friends, without whose insights it would not have been possible. He would also like to thank Eloise Cook, Saraswati Bannerjee and all the other editing staff at Pearson for their invaluable support and guidance.

Publisher's acknowledgements

Text credits:
2 U.S. Government Publishing Office: Private banking and money laundering: a case study of opportunities and vulnerabilities, U.S. government publishing office. **4 National Commission on Terrorist Attacks Upon the United States:** National Commission on Terrorist Attacks upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission p.140 (www.9-11commission.gov/staff_statements/911_TerrFin_Monograph.pdf) **14 FATF-GAFI:** FATF Report : Virtual Currencies – Key definitions and potential AML/CFT risks – June 2014 **15 FATF-GAFI:** Virtual Currencies: Guidance for a Risk Based Approach. FATF June 2015 **16 FATF-GAFI:** Virtual Currencies: Guidance for a Risk Based Approach. FATF June 2015 **20 European Union:** The financing of the 'Islamic State' in Iraq and Syria (ISIS), 11 September 2017, European Union **20 New York Times**

Company: Alderman, Liz. (2018) French Cement Giant Lafarge Indicted on Terror Financing Charge in Syria, June 28, 2018, The New York Times. **33 European Union:** © European Union, http://eur-lex.europa.eu/ **37 Crown Copyright:** UK Criminal Finances Act 2017 **66 Hearst Communications, Inc.:** Meyer, Philip. (1970) If Hitler asked you to electrocute a stranger, would you? February 1 1970, Hearst Communications, Inc. **84 FATF-GAFI:** www.fatf-gafi.org copyright © FATF/OECD. All rights reserved. **91 JMLSG:** JMLSG http://www.jmlsg.org.uk/download/9984 **93 The Wolfsberg Group:** The Wolfsberg Group www.wolfsberg-principles.com **94 The Wolfsberg Group:** The Wolfsberg Group www.wolfsberg-principles.com **96 The World bank Group:** Schott, P.A. (2003) Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism, World Bank/IMF, Chapter VI. **81 Trulioo:** How Financial Institutions Can Use AI to Enhance Due Diligence, MARCH 1, 2018, Trulioo **120 FATF-GAFI:** www.fatf-gafi.org copyright © FATF/OECD. All rights reserved. **127 FATF-GAFI:** www.fatf-gafi.org copyright © FATF/OECD. All rights reserved. **186 Financial Conduct Authority:** The UK's Financial Conduct Authority defines reputational risk **186 US Federal Reserve:** US Federal Reserve **187 The Financial Times Limited:** Arnold, Martin. (2014) HSBC wrestles with soaring costs of compliance, August 5 2014, The Financial Times Ltd **188 Danske Bank:** Bruun & Hjeijle which outlined the extent of the AML failings at Denmark's largest bank **190 KYC global technologies:** Riskscreen, Infographic – Deutsche Bank's $10 billion scandal: 'mirror trading' explained 17 Feb 2017 **190 Financial Conduct Authority:** Financial Conduct Authority **191 Andy Cecere:** Andy Cecere **193 The Art Newspaper:** Sansom, Anna. (2019) French court fines Art Basel backer UBS €3.7bn for tax evasion and money laundering, 20th February 2019, The Art Newspaper **196 mySociety Limited:** MacKinlay, Andrew (2009) Lloyds TSB and Iran (Sanctions), 12th February 2009, mySociety Limited **197 United States General Accounting Office:** Minority staff report for permanent subcommittee on investigations hearing on private banking and money laundering: a case study of opportunities and vulnerabilities, November 9, 1999, United States General Accounting Office **200 U.S. Government Printing Office:** Raul Salinas, Citibank, and Alleged Money Laundering, October 1998, U.S. Government Printing Office **199 United States Senate Committee on Homeland Security and Governmental**

Affairs: June 1993, Elliott emailed a colleague in Switzerland **201 United States Senate Committee on Homeland Security and Governmental Affairs:** June 1993, Elliott emailed a colleague in Switzerland **202 U.S. Government Printing Office:** Raul Salinas, Citibank, and Alleged Money Laundering, October 1998, U.S. Government Printing Office **203 U.S. Government Printing Office:** Raul Salinas, Citibank, and Alleged Money Laundering, October 1998, U.S. Government Printing Office **203 U.S. Government Printing Office:** Raul Salinas, Citibank, and Alleged Money Laundering, October 1998, U.S. Government Printing Office **204 U.S. Government Printing Office:** Based on facts from www.access.gpo.gov/congress/senate/pdf/109hrg/20278.pdf **230 JMLSG:** JMLSG Guidance 2017, Part I, 6.11 (from http://www.jmlsg.org.uk/ **293 Financial Action Task Force:** FATF report in January 2018 ('Financing of Recruitment for Terrorist Purposes') **305 Brian Jenkins:** 1996, Brian Jenkins, senior adviser to the President at the RAND Corporation and an internationally recognised expert on terrorism, noted three potential reasons for this trend **306 United Nations:** UN Convention Against Trans-National Organised Crime, 2000 (the Palermo Convention) **323 Incisive Business Media Limited:** Investment Week

Disclaimer

The content of this book is intended solely for educational purposes, to describe and explain key concepts, processes, laws and standards. It should not be relied upon for operational purposes and purchasers should take care to obtain local legal advice on all operational issues affecting their business.

To my father and mother, John and Valmai Parkman

Introduction

This book was conceived, designed and written primarily as a practical aide-memoire for all those who have to grapple with the money laundering and terrorist financing risks as part of their daily professional work. Its target audience, therefore, is not just Compliance Officers and Money Laundering Reporting or Prevention Officers in banks and other types of financial institutions, but also the increasing number of job roles which demand some knowledge of money laundering and terrorist financing risk and its countermeasures – CEOs and finance directors, auditors, internal controllers, risk managers, in-house counsel and corporate communications managers, as well as regulators, law-enforcement, business journalists, students, consultants and educators.

Assuming no prior knowledge of Anti-Money Laundering (AML) or Counter-Terrorist Financing (CTF) on the part of the reader, the book starts with an examination of fundamental terms and processes (Chapter 1) before going on to look at the international framework of legal and regulatory standards which has been developed over several decades (Chapter 2) and the necessary activities and organisation of an AML CFT Compliance function and its positioning within the wider framework of the organisation (Chapter 3). The book then gives a detailed play-by-play of how to design and implement a risk-based Customer Due Diligence (CDD) and Know Your Customer (KYC) programme (Chapter 4) and goes on to look at Reputational Risk (Chapter 5) Suspicion Recognition (Chapter 6) and International Cooperation (Chapter 7). The book concludes with two case studies which can be used for in-house staff training, covering key issues such as political exposure and corruption risk in clients and customers,

complex ownership structures, hidden beneficial ownership and methods of circumventing international risk-based controls.

To those returning to *Mastering Anti-Money Laundering and Counter-Terrorist Financing,* since the first edition of the book was published in 2012, there has been a range of developments which have exerted a significant effect on the overall landscape. A lot has happened or is set to happen. For example, legal and regulatory developments such as and many more.

- the EU 4th, 5th and 6th AML Directives
- developments in the interface between AML/CTF regulations and Data Protection/Data Privacy laws
- the advent in some jurisdictions of so-called 'Failing to Prevent' offences, mandatory corporate and real property beneficial ownership registers and disclosure requirements
- the expansion in tools for combating money laundering and corruption, such as Unexplained Wealth Orders (used in e.g. Ireland and Australia for a number of years but brand new for countries like the UK)
- the AML implications of MFID II
- the US Final Rule on Customer Due Diligence
- the latest developments and direction of travel in the battle against tax evasion through the OECD framework for the exchange of tax information and impactful national legislation such as US FATCA (Foreign Account Tax Compliance Act)

Then, when one moves beyond law and regulation to think about other developments in the wider world since 2012, one realises just how long ago it was. On the terrorism and terrorist financing side, ISIS had yet to make its first grisly appearances in Iraq and Syria, and in Europe there had been no Bataclan, no Brussels airport, no Manchester Arena. There had been no massacre at the Al Noor mosque in Christchurch, New Zealand.

'Bitcoin' and 'Blockchain' as terms of use had barely penetrated public consciousness, and few people outside of the FBI had heard of 'Silk Road' and the 'dark web'. Yet now, cryptocurrencies are starting to become almost mainstream, regulation is following (such as Gibraltar's licensing scheme for 'Distributed Ledger Technology Service Providers') and experts are talking seriously about whether or not fiat currencies may turn crypto and

lead to the abolition of formal cash. What effects will that have on the way in which we run our AML and CTF regimes?

I don't remember 'FinTec' being widely used as a term back in 2012, but now we're witnessing a massive growth in start-ups of new companies providing new ways of raising funds, investing, buying things and paying people, all driven by new technologies and all of which have significant implications for the fight against financial crime.

Talking of technology and its use in day-to-day AML Compliance departments, seven years ago was anybody doing 'dynamic risk assessment' (automated, real-time updating of customer risk profiles based on trigger events)? Was anybody actually using Artificial Intelligence (AI) to drive CDD and customer on-boarding processes or to reduce the false-positive ratios in their automated suspicion-reporting engines? They are now.

So much has changed and developed. But alas, one thing has remained frustratingly constant – the fines: Deutsche, Danske, ING, Rabobank, US Bancorp, Commonwealth Bank of Australia, Barclays and many, many more. Why are we still getting it so wrong? What can we do differently? What, if any, lessons have we learned these last seven years?

These are important questions because the problems are very big and, unfortunately, they seem to be getting worse. USD 2 trillion equivalent is paid in bribes worldwide to government officials according to various sources such as the IMF, the World Bank, the UN and the State Department. Another trillion is derived from activities such as narcotics, people-trafficking, counterfeit goods, smuggling and so on. It looks as if there may be upwards of USD 3–4 trillion equivalent of crime proceeds that need to be laundered, or roughly 3–4 per cent of global GDP, and the figures are going up, not down. For terrorism, the picture isn't any rosier. The number of attacks has been rising. And the number of countries experiencing attacks has been rising – for example 77 countries experienced terror attacks in 2017 compared with 66 in 2016.

In terms of the strategy for dealing with this, what we've done, as a planet, over the last 30 or so years is to construct an edifice or framework to try to prevent the systems of the world being used for the purposes of cleansing and normalising this illicit wealth. And that framework consists of four main pillars:

- **Pillar 1: Laws, Regulations and Penalties** – Example: Money Laundering and Terrorist Financing must be made criminal offences in your country. It's a criminal offence if you fail to report a suspicion of money laundering or terrorist financing; it's a criminal offence if you warn a customer that they're under investigation; You'll be fined heavily if your organisation's systems and controls aren't up to standard, etc.
- **Pillar 2: Institutions and Cooperation** – Example: You've got to have a Financial Intelligence Unit in your country to whom banks and other required business types must report suspicions. And they and your police, your prosecutors, your judges and your court officials must be well resourced and capable of dealing with these matters effectively and of cooperating, both with each other and with similar agencies in other countries.
- **Pillar 3: Processes and Technology** – Example: At the 'front end', you have to collect information on your clients to identify them and try to determine, effectively, how likely it is that they're a money launderer. If you're a bank, you should have watchlist screening systems and systems that flag up if a customer's transaction profile is significantly different to what you're expecting, etc. And finally;
- **People and Culture** – Example: In the financial industry we operate something called the 'Three Lines of Defence Model', in which customer-facing staff, as the first line of defence, are meant to be 'tuned in' and looking out for these risks both when they onboard clients and while managing the relationship going forward, with Compliance and Audit providing specialist advisory and assurance capabilities as the second and third lines of defence, respectively. Organisations are meant to develop a 'Compliance Culture', which must be led by senior management, who must set the 'Tone at the Top'.

So that is the 'big picture' of what we have built, and that is what is operating currently. But there's a problem with it. Unfortunately, it doesn't seem to be working very well. And I detect a growing sense, if not of failure, then at least of serious dissatisfaction at the results which are being achieved for all the effort that is being put in. I attended an event not so long ago, at which a senior representative from a large UK global bank informed the group that they now have 20,000 people working in

Compliance – many of them involved in CDD and KYC duties. That's roughly 10 per cent of their entire global workforce. A representative from a US bank then responded that she thought numbers like that were 'a bit on the low side' of what was probably required. At other end of the client management process, some transaction monitoring systems are producing 'false positives' (alerts which don't lead to anything) at rates well into the 90 per cent plus range – again with whole armies of people to analyse the output. People-heavy, manual, paper-based, expensive, repetitive, inefficient – it's costing the earth and the costs are going up.

This might be worthwhile – a necessary evil – if it was resulting in more prosecutions, more assets seized and less money laundering. But that doesn't seem to be the case. The estimates of laundered money go up, the asset seizure and conviction rates for criminals stay stubbornly low, the fines on banks get bigger and more frequent. Nobody's happy. An outgoing senior officer at Europol stated recently that they have identified 400 top, professional launderers wo are 'running billions through the banking system with a 99 per cent

success rate.' On top of this, the industry and law enforcement are grappling with new or rapidly changing techniques – trade-based money laundering and transaction laundering (such as the use of e-commerce platforms for goods, personal transport and accommodation services) to launder money. There are new technologies, platforms and products that are being used for these purposes – Distributed Ledger Technologies, Blockchain, cryptocurrencies such as Bitcoin and Ethereum, Initial Coin Offerings, Initial Token Offerings, crowd-funding, digi-cash, peer-to-peer direct transfer platforms. The rapid pace of change and the constantly evolving nature of the threats is unrelenting and threatens to overwhelm us, unless we can find a way to be more effective.

Of course, we don't have the counterfactual. We can't see what things would have been like on planet Earth regarding crime and money laundering if we hadn't put the structures described in this book in place. Who knows? It might be a lot worse than it is, in which case preventing that should register as an achievement. But I'll close this introduction with a -comparator – an unconnected example where serious attempts have been made to counter a perceived societal threat. Just over 50 or so years ago in the UK, as an example, in the mid-1960s, there were a million cars on the roads and there were 6,500 road deaths a year. In 2016 there were 36

million vehicles on British roads, and the death count was 1,600, a reduction rate which has been repeated in other countries which have adopted a coordinated approach to road safety. Now, clearly, there are limits to this analogy, but it is of course the case that the push to make the roads safer has involved some of the same 'pillar' types used to combat money laundering – Law and Penalties (drink drive laws, compulsory seatbelts, don't text while you're driving, 'we'll fine you, take your license away, send you to jail', etc.); Technology and Processes (safer cars, ABS braking, collision avoidance, speed cameras, black boxes, the points system and, pretty soon, driverless cars); and People and Culture (road safety adverts on TV, posters on our streets, and an attempt at genuine attitude change – drink driving, for example, is generally no longer considered to be socially or morally acceptable).

The returns in the fight against money laundering and terrorist financing, using similar strategies, have not been as good and we need to look to the future to see how we can make a better impact on the problem. As ever, technology offers a chance of making a real difference and the developments in the application of Artificial Intelligence (AI), machine-learning and blockchain described elsewhere in the book can perhaps help to turn the tide in a more positive direction. But it is unlikely to provide the entire answer and anyone thinking that we will ever be able to let the machines get on with fighting financial crime so that we human beings can get back to concentrating on making money is likely to be disappointed. In fact, not just disappointed but possibly criminalised, too. I predict that the Deferred Prosecution Agreement (DPA) protocol which has become the default model for 'punishing' financial institutions through the administration of increasingly massive financial penalties (but under which nobody – particularly at senior levels – ever goes to jail) isn't going to be allowed to continue producing such poor returns for very much longer. It will have to be supplemented with something altogether more fierce and threatening to the senior business leaders who set the targets and the tone within financial organisations, but who are at present protected from criminal liability because of their lack of direct involvement in the failures for which their organisations have been sanctioned. At some point in the future, governments looking to construct criminal cases against senior individuals in the wake of money laundering scandals will not be confined by a lack of proximity or specific intention on the part of their targets, but

will be able to look instead to wider seams of relevant behaviour on which to found criminal liability. For example, those which the management scientist Edgar Schein (*Organizational Culture and Leadership*, 5th edition, 2017) calls those 'primary embedding mechanisms' through which leaders influence the culture of their organisations, such as:

- what they pay attention to, measured and control on a regular basis (and, by extension of course, what they *don't*)
- how they react to critical incidents and organisational crises
- how they allocate resources
- how they role-model, teach and coach their colleagues
- how they allocate rewards and status; and
- how they recruit, select, promote, 'excommunicate' and fire their direct reports.

About the author

Tim Parkman
After graduating in Psychology and Philosophy from Oxford University and then studying law at the University of Central England, Tim qualified and worked in the litigation department of City of London law firm Wilde Sapte (now Dentons) before joining the Standard Chartered Banking Group where he held a number of senior operational legal and compliance positions in London, Singapore, India and the UAE.
Tim is the Managing Director of Lessons Learned Ltd, specialising in the provision of integrity and financial crime business education and consulting services internationally and a founder and director of CDD-Pro Ltd, a provider of software to improve the quality of customer onboarding information produced by front-line relationship managers. He is a member of the EBRD's panel of experts on Money Laundering and Terrorist Financing and is also the author of *Countering Terrorist Finance: A Training Handbook for Financial Services* (Ashgate).

1

Fundamental Concepts

Background and definitions

Key processes in money laundering and terrorist financing

Money laundering

Crypto-Laundering and the Blockchain

Terrorist financing

Further differences between terrorist financing and classical money laundering

Suspicion recognition

BACKGROUND AND DEFINITIONS

Definitions

Money laundering is the conversion or transfer of money to disguise its illegal origins; or the use of the financial system to convert or transfer money or other assets so as to disguise their illegal origins. (AML is the acronym used for Anti-Money Laundering.)

Terrorist financing is the use of the financial system to facilitate the funding of terrorist acts, and to disguise both the origins and intended purpose of the funds used. *Note:* The generally used acronym CFT has been used for Countering the Financing of Terrorism.

In historical terms, even though banks and other financial institutions have been used by criminals since the dawn of modern commerce for hiding, transferring money and disguising their source of wealth, the emergence of money laundering and terrorist financing as a bank risk in its own right has been relatively recent.

One can distinguish between *money laundering and terrorist financing risk* on the one hand, and *Know Your Customer (KYC) and regulatory risk* on the other. The first is the risk that a financial institution will actually be used as a conduit for criminally derived money, or for money that turns out to have been destined for a terrorist purpose. The second is the risk that, without having actually handled criminal or terrorist funds (or at least without having been proven to have done so), a financial institution will nevertheless be deemed to have been negligent or in some other way sub-standard in its adoption and enforcement of adequate policies and procedures designed to prevent actual usage of its facilities occurring.

This distinction is important because it impacts upon the *reputational* risks faced by financial institutions. Money laundering can be difficult to identify, terrorist financing even more so. Accordingly, the mere presence of criminal or terrorist funds within a financial institution will rarely be sufficient to attract censure or punishment. It must usually be accompanied

by an individual or corporate failure in expected standards. The counterpoint is that, conversely, a failure in standards *is* usually sufficient to attract censure or punishment, along with attendant reputational damage, even *without* the actual presence of criminal/terrorist funds within the organisation, although clearly it will be much worse when both elements are present.

Example

Amy Elliott was a vice president and senior relationship manager with the Citibank private bank during the 1990s, based in New York. Raul Salinas, the brother of the former President of Mexico, Carlos Salinas (and hence a Politically Exposed Person (PEP)), was introduced to her by a longstanding client of the private bank, Carlos Hank Rohn. Elliott opened multiple accounts for Salinas and his wife in London and Switzerland, using a variety of measures to ensure maximum confidentiality, such as code name accounts, offshore trust company accounts and a unique funds transfer method which succeeded in moving funds to these accounts from Mexico without creating any documentary evidence identifying Salinas as the owner of the funds.

Based on her knowledge of the region, and on her general perceptions of the Salinas family, Elliott made assumptions about the legitimacy of Salinas' wealth which later proved to be unfounded. With her supervisors looking on, she made no independent checks on the sources of his wealth and waived all references other than the one given by Carlos Hank Rohn. Later on, after Salinas had been arrested on suspicion of murder and after the Swiss authorities had frozen all the accounts and brought charges for laundering the proceeds of illicit narcotics trafficking, the case was the subject of hearings by the US Senate Committee on Investigations and

Elliott was questioned on the issue of what enquiries she had made about the origins of the money going through the accounts. An excerpt appears below.

Senator Levin: Now, did you know the source of his funds? Did you ask him the source of his funds? Let us put it that way.
Ms Elliott: Source of funds is where the money is coming from, and I knew two things. I knew that for his personal account the funds were going to be approximately $100,000, and it was going to come from one of the Mexican banks. And he told me it was going to be either Bancomer or Banca Cremi. He did not know which one.
Senator Levin: All right. Now, when he deposited the money later on. . .
Ms Elliott: Excuse me?
Senator Levin: When he deposited the millions later on, because it says here, 'and thereafter', did you know the source of those millions that he deposited later on?
Ms Elliott: I knew they were coming from Mexican banks.
Senator Levin: But did you know the source of his funds, where he got the funds from?
Ms Elliott: I believed at the time, Senator, that we were talking about monies that were a combination of things . . .
Senator Levin: Did you also believe that he had sold a construction company?
Ms Elliott: I did.
Senator Levin: And did you know the name of the construction company?
Ms Elliott: I do not.
Senator Levin: Did you ask him?

Ms Elliott. I did not.

Senator Levin: Did you ask him how much he received from the construction company?

Ms Elliott: I did not, sir.

Senator Levin: Did you ask him about any projects that that alleged construction company had ever undertaken?

Ms Elliott: Carlos Hank told me that they had worked on a road together . . . .

Source: http://www.gpo.gov/fdsys/pkg/CHRG-106shrg61699/html/CHRG-106shrg61699.htm

Compare this example with the situation involving those US banks that opened accounts for some of the 9/11 hijackers after they had arrived in the United States and were planning their attacks. The National Commission on the Terrorist Attacks upon the United States described their involvement as follows:

Example

'All of the hijackers opened accounts in their own name, using passports and other identification documents. Contrary to numerous published reports, there is no evidence the hijackers ever used false Social Security numbers to open any bank accounts. In some cases, a bank employee completed the Social Security number field on the new account application with a hijacker's date of birth or visa control number, but did so on his or her own to complete the form. No hijacker presented or stated a false number . . .

The hijackers' transactions themselves were not extraordinary or remarkable. The hijackers generally followed a pattern of occasional large deposits, which they accessed frequently through relatively small ATM and

debit card transactions. They also made cash withdrawals and some occasionally wrote checks. In short, they used their accounts just as did many other bank customers. No one monitoring their transactions alone would have had any basis for concern . . . Even in hindsight, there is nothing . . . to indicate that any SAR [Suspicious Activity Report] should have been filed . . . .'

Source: *National Commission on Terrorist Attacks upon the United States: Monograph on Terrorist Financing, Staff Report to the Commission* p.140 (www.9-1commission.gov/staff_statements/911_TerrFin_Monograph.pdf)

The effect of this distinction is that financial institutions need to pay very close attention, *in advance* of any problems, to the issue of how their policies and standards (and just as importantly their adherence to those policies and standards) will stand up to scrutiny *if* it turns out that there is a problem subsequently.

KEY PROCESSES IN MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering and terrorist financing bear many similarities, but there are some key distinctions.

With non-terrorist criminal money laundering, the funds in question always have a criminal origin. The process has been described as having three distinct phases.

- *Placement*: the moment at which criminally obtained cash is first 'dematerialised' and put into the financial system (e.g. as a credit entry on a bank account).NB This phase isn't necessary where the crime in question is not cash generative – e.g. fraud or tax evasion.
- *Layering*: the movement of the money through a large series of transactions with no real economic purpose, in order to make it more

difficult to prove the criminal origin of the funds and disguise ownership.

- *Integration*: the eventual use of the money for a genuine economic purpose (e.g. the purchase of a luxury item or a business capable of generating further profits from legitimate business activities).

With money laundering, the basic aim is to hide the criminal origin of the funds. The amounts in question are typically large and hence easier to detect.

With terrorist financing, the key difference is that the funds passing through the financial system *need not* have a criminal origin, even though quite often they do. They can stem from a variety of different sources, many of them legitimate at the point of acquisition.

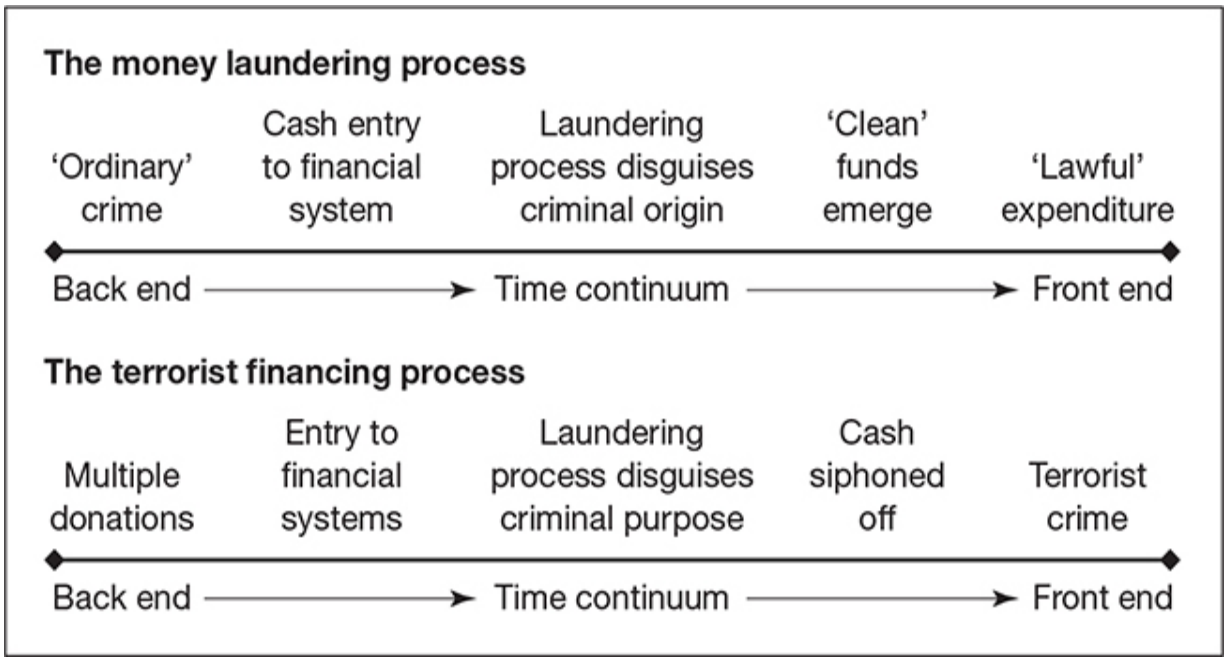
A particular feature of terrorist financing (and not just so-called 'Islamist' terrorist financing, but extending to other groups as well over the past few decades) is the use of non-profit, charitable, religious or cultural organisations as 'cover' for the passage of funds.

With terrorist financing, the basic aim is to hide the criminal *purpose* of funds. By the time funds have been designated and made available for a specific terrorist attack, the amounts in question are typically quite small and hence harder to detect.

The key differences between money laundering and terrorist financing processes are represented diagrammatically in Figure 1.1.

Perhaps the most important difference between the two is between the people who undertake each activity. Money laundering is done by criminals – particularly those involved in organised crime. Their goal is solely to enrich themselves, essentially the more the better. They are trying to wash as much money as possible through the system. Terrorists are different people with different motivations, being either genuinely committed to a religious, ideological or political cause to the point of being prepared to kill innocents in pursuit of it , or 'brainwashed' into doing so and being prepared to use the financial system in the funding of their campaign of violence.

Figure 1.1 **The key differences between the two processes**



MONEY LAUNDERING

Money launderers use various elements of the financial and commercial system for their activities.

Transportation and consolidation

This is basically the conversion of criminal cash into larger denomination notes. Large amounts of small currency (coins or notes) derived from crime are difficult to manage and very difficult to transport from one physical location to another. A smaller amount of large denomination notes is much easier to handle and can be more easily concealed if, for example, the money launderers want to smuggle it across borders to be laundered in other countries.

Customers who appear regularly to be exchanging large amounts of small currency units for much larger denominations and who do not appear to have any logical reason for doing this might well be cause for suspicion.

Placement

Placement involves the various methods used by money launderers to dematerialise their criminal money within the financial system.

One method involves the use of ‘smurfs’. The money launderer gives a sum of cash to an individual known as a ‘smurf”. The ‘smurf’ deposits the cash in small amounts into a number of different bank accounts, probably held at several different banks. The deposit amounts are small enough that they do not attract attention or suspicion. Once the money is deposited, the placement stage is complete.

A second method involves the use of ‘front companies’. The launderer selects company and business bank accounts belonging to apparently respectable, high net worth individuals. The money launderer gives a much larger sum of cash to these people. The cash is then paid into their accounts and, with the support of forged documentation, is explained as a legitimate receipt from the sale of a property or the sale of an interest in a business for example. Once the cash is deposited and the purpose of the transaction successfully explained, the placement stage is complete.

Any business that is cash intensive is useful, since it already handles large amounts of legitimate cash, and the criminal cash can be mingled with this and banked as if it were the legitimate proceeds of the business. Examples of cash intensive businesses include supermarkets, restaurants and jewellery shops.

Yet another method involves the purchase of different types of insurance and investment policies for cash, through independent financial advisers or brokers who have persuaded themselves that the cash is of legal provenance. At a selected moment, the policy is surrendered and a redemption cheque or funds transfer is received from the issuer. Or the cash can be exchanged for bitcoins or other virtual currencies, using e-wallets and bitcoin exchange services.

Ultimately, amounts so ‘placed’ in apparently legitimate accounts held by other people may then be transferred to a single account which acts as a

conduit for the money as it is moved on elsewhere, as part of the layering process described below.

Layering

This is essentially the technique used by money launderers to process their money in such a way as to disguise its connection with crime. There are a number of possible examples:

- investment in financial products which have good liquidity and which can be bought and sold easily (e.g. unlisted stocks and shares)
- purchase and sale of real estate – apartments, houses, flats, commercial premises
- transfer of the money to a business, ostensibly as a 'loan' with documents such as loan agreements and receipts to support the illusion that the loan is real
- transfer of the money overseas or to other accounts under the guise of money destined for a specific purpose (e.g. education overseas of a family member)
- using fictitious business transactions to move money around (e.g. giving money to suppliers against invoices raised for goods that were never issued; or raising invoices to customers in respect of sales that never took place)
- transferring money to companies overseas in payment for non-existent shipments of imported goods
- use of shell companies and shell banks, i.e. entities that have no real function, no real place of business and no real business operations, but which exist in name only as a conduit for the receipt and distribution of money
- use of the international financial markets to buy and sell securities and move money across international borders.
- conversion of funds into cryptocurrencies such as Bitcoin and Monero through an exchange, conducting crypto transactions and investments, and then re-converting the assets into fiat currency. (See later in this chapter for more detail on the use of cryptocurrencies in money laundering.)

Use of criminally owned or sympathetic investment firms and banks

Investment business and banking gives money launderers an opportunity to move large amounts of money into the international financial markets. The high turnover of such markets (customers might legitimately buy and sell many times in any one day) is useful in helping the money launderers to move their money around as much as possible.

Investment firms will legitimately transact very large volumes of purchase and sale deals in any one day. A criminally owned investment firm can, of course, use its business systems and resources to launder large amounts of criminal money through large-scale transactions.

Use of shell companies and shell banks within the overall laundering process

Shell companies have no purpose other than to act as a conduit for money. Money launderers will use shell companies as a vehicle for their money movements; as somewhere where money can be received and co-mingled with other funds, before it is transferred on to another destination.

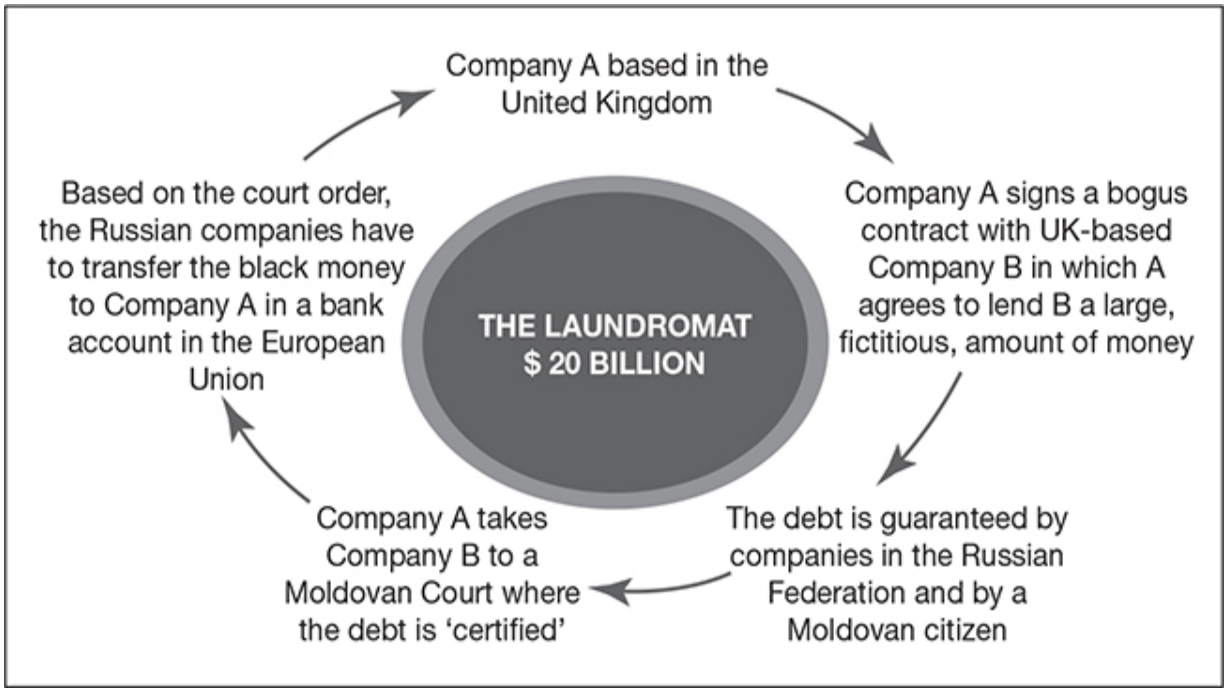
Any activity which appears to have no real economic purpose should be an immediate cause for suspicion. Any activity which does not match your - understanding of a customer's likely needs and which does not seem plausible for that particular customer should also give you cause to be suspicious.

Example

The Russian Laundromat

Exposed by the Organized Crime and Corruption Reporting Project (OCCRP) in 2014, the so-called Russian Laundromat was a scheme which apparently succeeded in laundering more than USD 20 billion out of Russia, using many of the above features, but crafted into a very particular and notable methodology shown in Figure 1.2.

Figure 1.2 **The Russian Laundromat**


Company A based in the United Kingdom
Company A signs a bogus contract with UK-based Company B in which A agrees to lend B a large, fictitious, amount of money
The debt is guaranteed by companies in the Russian Federation and by a Moldovan citizen
Company A takes Company B to a Moldovan Court where the debt is 'certified'
Based on the court order, the Russian companies have to transfer the black money to Company A in a bank account in the European Union
THE LAUNDROMAT
$ 20 BILLION

Launderers created a core of 21 companies based in the United Kingdom (UK), Cyprus and New Zealand which were run by hidden owners. A number of Russian companies then used these companies to move their money out of Russia.

To get the money out, the scheme's organisers devised a clever misdirection. They created a fake debt among some of these core shell companies and then got a Moldovan judge to order the Russian company seeking to launder funds to pay that debt to a court-controlled account. Moldindconbank in Moldova held those accounts. The companies involved in the fake debt also had accounts at the same bank. Soon, Moldindconbank was deluged with funds sent in from the Russian companies. About $8 billion was then withdrawn directly from these accounts in Moldova and sent around the world.

Meanwhile, nearly $13 billion more was transferred to Trasta Komercbanka in Latvia. Some of the money disappeared into the maze of these same shell company accounts. Trasta Komercbanka's location in the European Union made the transactions less likely to be questioned by other banks. The money was now considered 'clean' 'European' money that could be spent on anything the Russians wanted.
(https://www.occrp.org/en/laundromat/the-russian-laundromat-exposed/)

Non-cash laundering

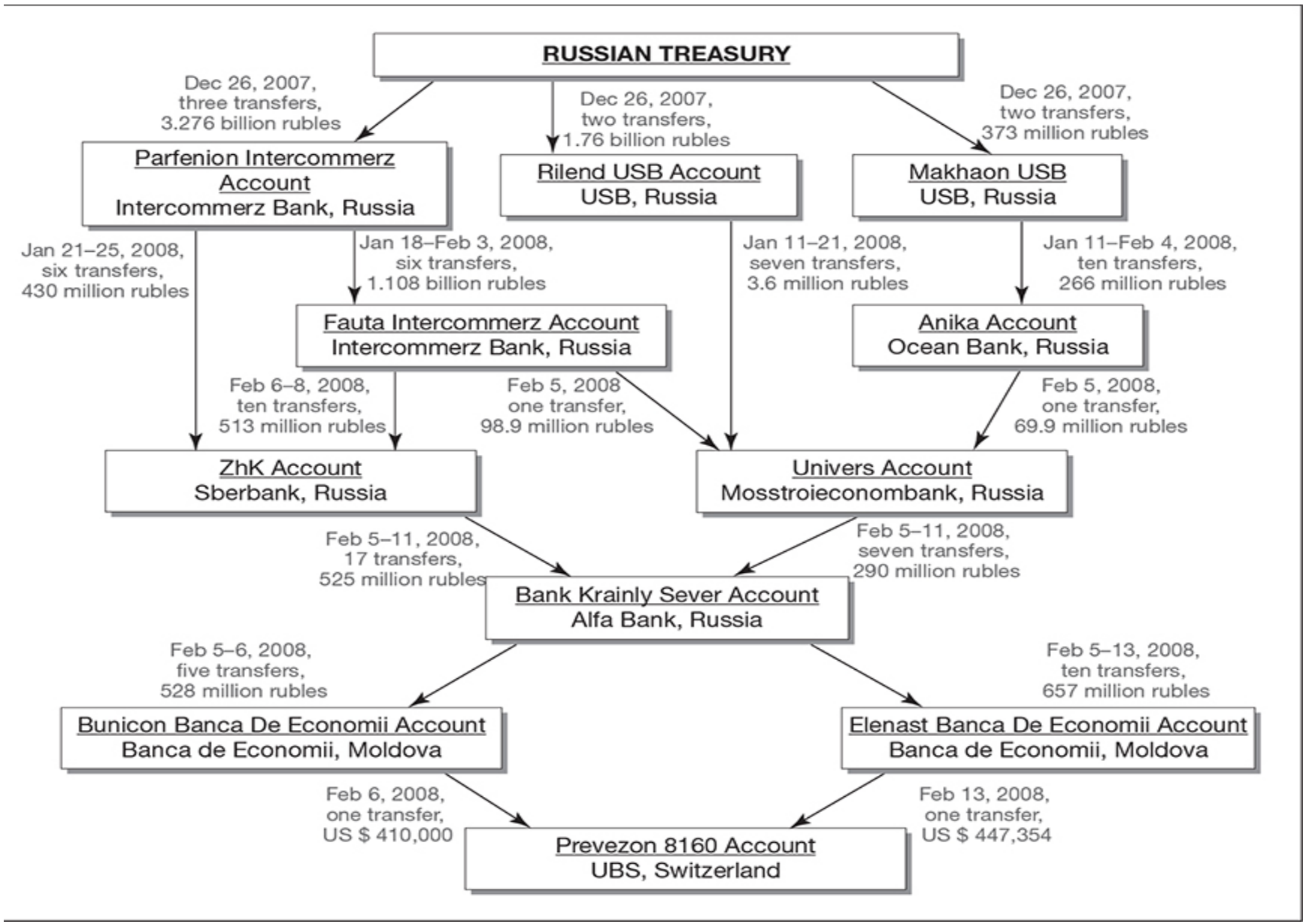
While classic money laundering models emphasise the role of cash at the Placement stage, it's important to remember that any crime that produces criminal proceeds can generate money laundering activity, regardless of whether or not cash is involved. So, for example, the proceeds of fraud, corruption, tax evasion and other crimes not necessarily (and, in fact, not usually) involving cash will need to be laundered through the financial system in order to disguise their criminal origin and immunise their criminal owners against successful prosecution and punishment. Indeed, given the amounts estimated to be paid in bribes to public officials for the award of contracts (recently estimated by the World Bank at USD 1.5 trillion annually) it is clear that a very significant amount of global money laundering by value will not actually involve cash crimes.
Despite the absence of large amounts of cash, however, schemes for laundering the proceeds of fraud and corruption still utilise various features of the middle and later stages of the laundering process. The case described below has become highly politicised, due to the Russian government's -sensitivities of criticisms levelled at it by the company's owner, the Anglo-American fund manager, Bill Browder, and its denials of the key charges. But on the basis of *res ipsa loquitur* (a thing speaks for itself) it is included below, as it does illustrate in particular the use of multiple banks and the splitting of initial sums into multiple different 'layers' as part of a laundering scheme.

Example

The Magnitsky Case

Hermitage Asset Management had its corporate seals stolen during a raid on its Moscow offices by the Moscow police. These seals were then used to make a fraudulent 250 million dollar equivalent tax rebate claim to the - Russian tax office, a claim which was actually paid to the fraudsters by corrupt officials inside the tax office. The stolen money was then laundered out of Russia (see Figure 1.3) and used to purchase properties and luxury items in desirable locations such as Dubai and Manhattan and for the officials in question. Hermitage hired a Russian lawyer, Sergei Magnitsky, to investigate the case. Magnitsky was promptly arrested by the people he was investigating. He was imprisoned, tortured and died in jail. The Sergei Magnitsky Act was then passed into law by the US Congress, containing a travel ban against the suspect officials, following which the Russian Duma then passed in retaliation its own law banning the adoption of Russian children by United States citizens. Magnitsky himself was then posthumously convicted of tax fraud in Russia. A man called Alexander Perepilichnaya, who had provided evidence to the authorities concerning the money laundering route out of Russia, was found dead outside his home in Surrey, England, in November 2012, the fourth person connected to the case to have died in suspicious circumstances, although a British coroner found in December 2018 that he had died 'of natural causes'.

Figure 1.3 **Magnitsky case: The movement of stolen funds out of Russia**


RUSSIAN TREASURY
Dec 26, 2007, three transfers, 3.276 billion rubles
Dec 26, 2007, two transfers, 1.76 billion rubles
Dec 26, 2007, two transfers, 373 million rubles
Parfenion Intercommerz Account Intercommerz Bank, Russia
Rilend USB Account USB, Russia
Makhaon USB USB, Russia
Jan 21–25, 2008, six transfers, 430 million rubles
Jan 18–Feb 3, 2008, six transfers, 1.108 billion rubles
Jan 11–21, 2008, seven transfers, 3.6 million rubles
Jan 11–Feb 4, 2008, ten transfers, 266 million rubles
Fauta Intercommerz Account Intercommerz Bank, Russia
Anika Account Ocean Bank, Russia
Feb 6–8, 2008, ten transfers, 513 million rubles
Feb 5, 2008 one transfer, 98.9 million rubles
Feb 5, 2008, one transfer, 69.9 million rubles
ZhK Account Sberbank, Russia
Univers Account Mosstroieconombank, Russia
Feb 5–11, 2008, 17 transfers, 525 million rubles
Feb 5–11, 2008, seven transfers, 290 million rubles
Bank Krainly Sever Account Alfa Bank, Russia
Feb 5–6, 2008, five transfers, 528 million rubles
Feb 5–13, 2008, ten transfers, 657 million rubles
Bunicon Banca De Economii Account Banca de Economii, Moldova
Elenast Banca De Economii Account Banca de Economii, Moldova
Feb 6, 2008, one transfer, US $ 410,000
Feb 13, 2008, one transfer, US $ 447,354
Prevezon 8160 Account UBS, Switzerland

Integration of laundered assets into the legitimate economy and repatriation to the home territory

Once the proceeds of criminal activity have been transported, consolidated, placed and layered they will, by the end of the process, have all the appearance of legitimately earned wealth, which can then be integrated into the legal economy. This could be done, say, through an investment in a business that produces a legally earned dividend or in a work of art or other item of intrinsic value which can either be enjoyed for what it is or sold. Investment income or sale proceeds may now be repatriated back into the country where the crimes were committed, so that they are available there to the ultimate criminal beneficial owner.

At a certain point in a person's life, he or she may decide to give up the criminal life, seek respectability and even political office, whereupon the powers of the state can then be used to legalise or pardon past acts and confer legitimacy on the criminal and those with whom he or she has consorted.

CRYPTO-LAUNDERING AND THE BLOCKCHAIN

Over the last five to seven years, so-called cryptocurrencies such as Bitcoin and Ethereum have rocketed to prominence in public consciousness, along with the new technology on which they are based – Blockchain. While no-one is in any doubt about the revolutionary long-term beneficial effects of Blockchain, questions still abound about cryptocurrencies, which continue to be cast across a range of characterisations from 'money launderers' best friend', through to 'the end of money laundering as we know it.' And the fast-moving nature of developments in the field can make today's comments out of date by tomorrow. That notwithstanding, the following is an attempt to summarise the background fundamentals of Blockchain and

crypto and explain how they can be used both to facilitate money laundering schemes and perhaps, in the future, to prevent them.

Blockchain

Blockchain is a technology which enables the creation and maintenance of 'de-centralised ledgers' which are both (a) secure, yet also (b) not controlled by a central ledger-keeping authority. The ledgers in question are records of transactions and ownership, and they can pertain to almost anything in this world that can be acquired, bought, owned, sold, preserved, improved and destroyed – books, houses, medical records, works of art, intellectual property rights and, of course, money.

A full account of how a Blockchain works is beyond both the scope of this book and the competence of the author, but some brief concept knowledge does help in understanding the potential money laundering implications discussed immediately after. Taking the idea of money (say, US dollars) as an asset which can owned, transferred and laundered, the traditional model for storing and transferring money is through a centralised ledger, depicted in Figure 1.4. In this model, all transactions are passed through a central party – such as a bank – which maintains the ledger of ownership as between the account holders.

The costs of centralised ledgers, however, can be significant, as not only will the central party charge for its services (thus increasing transaction costs), but it is also vulnerable to cyber-attack and operational risks such as IT failures, human error, bribery, etc. The solution to these weaknesses, therefore, comes in the form of a decentralised ledger, depicted in Figure 1.5, employing Blockchain technology, which removes the central party and either reduces or eliminates agency costs and the operational risks referred to.

Under such systems, users of the ledger (or rather the computers of users) are independent nodes within a Blockchain which, however, act collectively for the common verification of the ledger. Statements of account and changes to statements of account (such as occur, say, when transactions are made) are verified using cryptographic protocols which, it is commonly said, are effectively invulnerable to hacking and unauthorised use. (For an excellent description of how Blockchain works, which is suitable for non-

technical readers, see Daniel Drescher's *Blockchain Basics: A Non-Technical Introduction in 25 Steps,* Apress 2017.)

Figure 1.4 **Centralised ledger model**

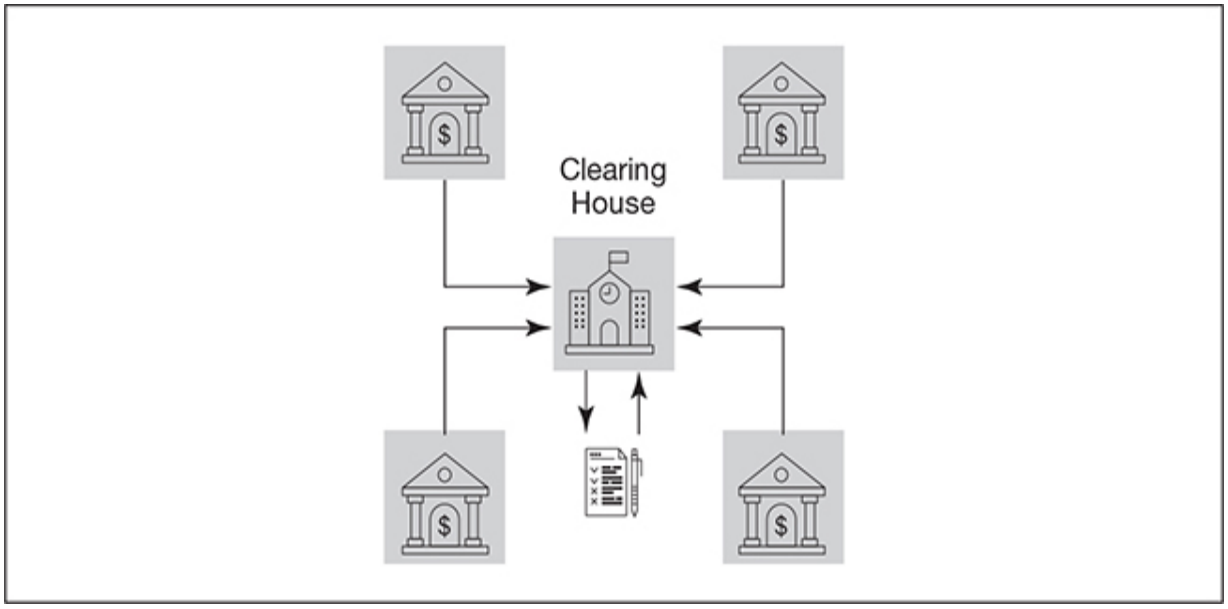
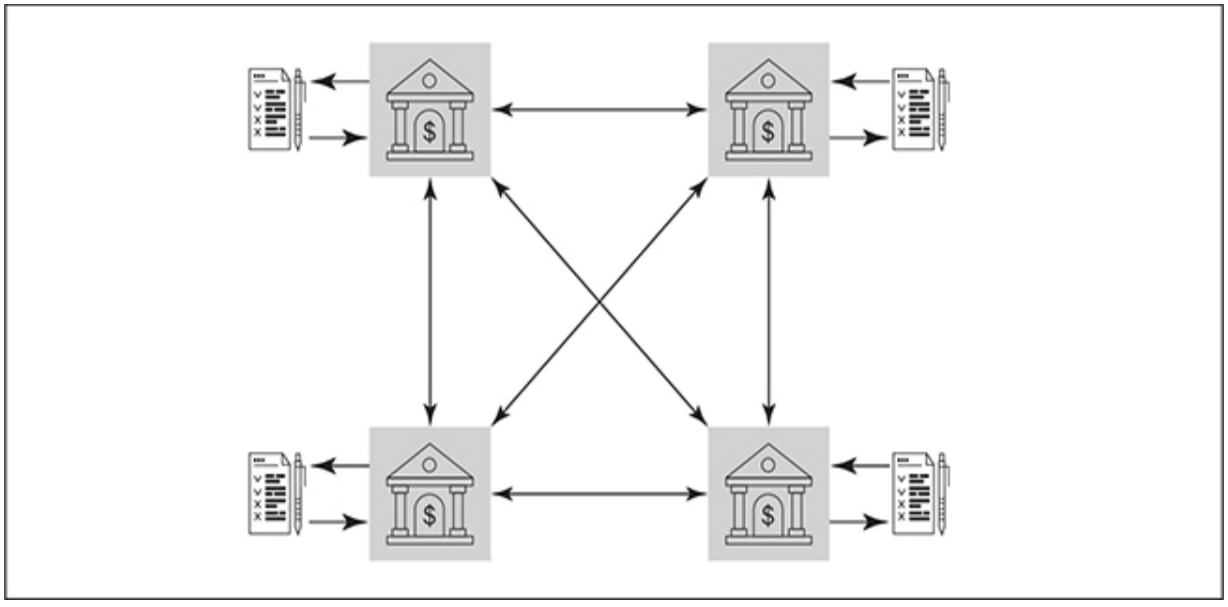


Figure 1.5 **Decentralised ledger model**



The first use of decentralised ledgers and Blockchain came not with regular fiat currencies issued by governments (pounds, dollars, euros, etc.) but with the cryptocurrency Bitcoin. The Financial Action Task Force (FATF) describes a cryptocurrency as

> **'a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. A decentralised virtual currency is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.' (See FATF Report: Virtual Currencies – Key definitions and potential AML/CFT risks – June 2014)**

Certain features of virtual currencies have made them attractive to criminals and money launderers:

- they may allow greater anonymity than traditional non-cash payment methods, as they can be traded on the internet in non-face-to-face relationships which, in turn, permit the anonymous funding of illicit activities
- they may also permit anonymous transfers due to the lack of formal identification of sender and recipient
- they allow almost instantaneous global reach and greater anonymity than traditional electronic money-based products. For example, Bitcoin protocol does not require or provide identification and verification of participants or generate historical records of transactions that are necessarily associated with real-world identity
- they rely on complex infrastructures that involve several entities, often spread across several countries, to transfer funds or execute payments making policing and monitoring transactions extremely difficult
- the use of additional software and anonymisation techniques (such as 'mixers' and 'scramblers') can obscure the source of a virtual transaction and facilitate anonymity
- there is no central oversight body, hence there is no centrally deployed monitoring system which can identify suspicious transactions

and

- it is hard for law enforcement to identify one central location for investigative or asset seizure purposes.

There have been a number of high-profile criminal cases involving - cryptocurrencies and money laundering in recent years, two of which are summarised below.

Example

The Silk Road Case

In September 2013, the US Department of Justice unsealed a criminal complaint charging the alleged owner and operator of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs, weapons, stolen identity information and other unlawful goods and services anonymously and beyond the reach of law enforcement, with narcotics trafficking, computer hacking, and money laundering conspiracies. The Justice Department also seized the website and approximately 173,991 bitcoins, worth more than USD 33.6 million at the time of the seizure, from seized computer hardware. The individual was arrested in San Francisco in October and indicted in February 2014; the investigation is ongoing. Launched in January 2011, Silk Road operated as a global black-market cyber bazaar that brokered anonymous criminal transactions and was used by several thousand drug dealers and other unlawful vendors to distribute unlawful goods and services to over a hundred thousand buyers, a third of whom are believed to have been in the United States. It allegedly generated total sales revenue of approximately USD 1.2 billion (more than 9.5 million bitcoins) and approximately USD 80 million (more than 600,000 bitcoins) in commissions for Silk Road. Hundreds of millions of dollars were

laundered from these illegal transactions (based on bitcoin value as of dates of seizure). Commissions ranged from 8 to 15 per cent of total sales price. Silk Road achieved anonymity by operating on the hidden Tor network and accepting only bitcoins for payment. Using bitcoins as the exclusive currency on Silk Road allowed purchasers and sellers to further conceal their identity, since senders and recipients of peer-to-peer (P2P) bitcoin transactions are identified only by the anonymous bitcoin address/account. Moreover, users can obtain an unlimited number of bitcoin addresses and use a different one for each transaction, further obscuring the trail of illicit proceeds. Users can also employ additional 'anonymisers,' beyond the tumbler service built into Silk Road transactions (see discussion below). Silk Road's payment system functioned as an internal Bitcoin bank, where every Silk Road user had to hold an account in order to conduct transactions on the site. Every Silk Road user had at least one Silk Road Bitcoin address (and potentially thousands) associated with the user's Silk Road account, stored on wallets maintained on servers controlled by Silk Road. To make a purchase, a user obtained bitcoins (typically through a Bitcoin exchanger) and sent them to a Bitcoin address associated with his or her Silk Road account to fund the account. When a purchase was made, Silk Road transferred the user's bitcoins to an escrow account it maintained, pending completion of the transaction, and then transferred the user's / buyer's bitcoins from the escrow account to the vendor's Silk Road Bitcoin address. As a further step, Silk Road employed a 'tumbler' for every purchase, which, as the site explained, 'sen[t] all payments through a complex, semi-random series of dummy transactions . . . – making it nearly impossible to link your payment with any [bit]coins leaving the site.' The founder of the site, Ross Ulbricht, (AKA 'Dread Pirate Roberts') was convicted of money laundering, computer hacking, conspiracy to traffic fraudulent identity

documents, and conspiracy to traffic narcotics by means of the internet in February 2015. He is currently serving a double life sentence plus 40 years without the possibility of parole. The US Court of Appeals for the Second Circuit upheld the conviction and sentence in May 2017 and the US Supreme Court declined to hear a further appeal in June 2018.

Virtual Currencies: Guidance for a Risk Based Approach. FATF June 2015

Example

The Liberty Reserve Case

In what is to date one of the largest online money laundering cases in history, in May 2013, the US Department of Justice charged Liberty Reserve, a Costa Rica-based money transmitter, and seven of its principals and employees with operating an unregistered money transmitter business and money laundering for facilitating the movement of more than USD 6 billion in illicit proceeds. In a coordinated action, the Department of the Treasury identified Liberty Reserve as a financial institution of primary money laundering concern under Section 311 of the USA PATRIOT Act, effectively cutting it off from the US financial system.

Established in 2006, Liberty Reserve was designed to avoid regulatory and law enforcement scrutiny and help criminals distribute, store and launder the proceeds of credit card fraud, identity theft, investment fraud, computer hacking, narcotics trafficking and child pornography by enabling them to conduct anonymous and untraceable financial transactions. Operating on an enormous scale, it had more than a million users worldwide, including more than 200,000 in the United States, and handled approximately 55 million transactions, almost all of which were illegal. It had its own virtual

currency, Liberty Dollars (LR), but at each end, transfers were denominated and stored in fiat currency (US dollars). To use LR currency, a user opened an account through the Liberty Reserve website. While Liberty Reserve ostensibly required basic identifying information, it did not validate identities. Users routinely established accounts under false names, including blatantly criminal names ('Russia Hackers,' 'Hacker Account,' 'Joe Bogus') and blatantly false addresses '123 Fake Main Street, Completely Made Up City, New York'). To add a further layer of anonymity, Liberty Reserve required users to make deposits and withdrawals through recommended third-party exchangers – generally, unlicensed money transmitting businesses operating in Russia, and in several countries without significant governmental money laundering oversight or regulation at that time, such as Malaysia, Nigeria and Vietnam. By avoiding direct deposits and withdrawals from users, Liberty Reserve evaded collecting information about them through banking transactions or other activity that would create a central paper trail. Once an account was established, a user could conduct transactions with other Liberty Reserve users by transferring LR from his or her account to other users, including front company 'merchants' that accepted LR as payment. For an extra 'privacy fee' (75 US cents per transaction), users could hide their Liberty Reserve account numbers when transferring funds, making the transfers completely untraceable. After learning it was being investigated by US law enforcement, Liberty Reserve pretended to shut down in Costa Rica but continued to operate through a set of shell companies, moving millions through their accounts in Australia, Cyprus, China, Hong Kong, Morocco, Russia, Spain and elsewhere.

In January 2016, the founder of the site, Arthur Budovsky, pleaded guilty to one count of conspiring to commit money laundering and on 6 May 2016, he was sentenced to 20 years in prison.

Because of the anonymity features of transactions *within* the Blockchain referred to above, regulatory approaches to risk management, in keeping with FATF's approach, are focusing on guarding the interfaces (such as exchange houses) between the fiat world and the virtual world, at which conversions and reconversions take place. Chapter 2 contains some current summaries of such regulatory approaches, although it is a rapidly developing area.

Whatever features that cryptocurrencies such as Bitcoin, Ethereum, Monero and the others have which may make money laundering easier along the lines described above, one that they definitely *don't* have when compared with ordinary, non-virtual money is arguably the most important one – fungibility. Just like a pint glass of water poured into a one-gallon container that is already half-full, cash that is deposited into a bank account is 'fungible'. If you pay £10,000 of cash into a bank account already containing £50,000 and then wire transfer £8,500 to a third party account, the £8,500 is not treated as being legally synonymous with the cash which you paid in, just as a pint of water poured from the container would not be 'the same water' that you poured in from the glass. In some ways, the whole concept of 'layering' as a stage in the money laundering process is based on this premise; you can't identify specific 'pieces of money' as being of criminal origin, because real money is fungible – one unit or sub-unit of it is legally indistinguishable from another. But cryptos are different. True to the logic-based cyber-world from which they are born, each crypto-coin – or part of a crypto-coin – has a distinct identity. It is unique – and unique things can be traced, with the right technology.

If, as has been suggested, governments did away with cash and started issuing fiat currency in digital form, it's possible that for every person born the day after, it would be possible to identify and tag every pound, dollar, euro, etc. that they ever earned and spent throughout their lives, as well as how and where they earned it and what they spent it on. In such a world (and without delving here into the privacy and liberty arguments which may yet prevent it) the positions of non-digital and digital currencies would effectively have been reversed, with fiat digital being the mainstream method of counting, storing and transferring value, and forms of non-

digital, non-fiat money having become the murky, distrusted coinage of people and transactions considered to be operating at the edges of the legal economy. The end of mainstream money laundering?

TERRORIST FINANCING

It is possible to discern two strands of terrorist financing, which occur at different ends of the chain shown in Figure 1.1. Type 1 terrorist financing refers to the financing of a terrorist movement over time, while Type 2 refers to the funding of specific attacks.
Over many decades, terrorist groups such as ISIS, Al-Qaeda, Jemaal - Islamiyah, the Liberation Tigers of Tamil Eelam (the LTTE or 'Tamil Tigers') and the Provisional IRA have all used the financial and commercial system in similar ways to fund their activities.

Type 1 terrorist financing

The methods used to obtain, collect and/or disguise funds for terrorist movements or causes have included:

- donations from charities sympathetic to the terrorists' cause (or possibly even set up by the terrorist group itself), or from charities whose administration systems have been infiltrated and 'hijacked' by terrorists who then divert legally obtained charitable donations to their own terrorist cause
- criminal activities including drug trafficking, the seizure of mines and oil wells and consequent sale of their outputs, people trafficking and forced prostitution, gun running, counterfeiting operations, fraud, identity theft, etc.
- voluntary payments from ethnic diaspora (both legal expatriates and illegal immigrants)
- funds extorted from ethnic diaspora under threat of exposure to the immigration authorities or harm to their families

- legitimate business activities carried out by front companies, or 'donor' businesses sympathetic to the terrorists' cause
- where military success permits the creation of a 'proto-state' (see the comments on ISIS later in this chapter), exploitation of the economic resources of the controlled area from, e.g. the sale of natural resources and the levying of general taxation.

Type 2 terrorist financing

The methods used to fund specific terrorist attacks have included:

- ATM and credit card withdrawals on personal accounts – used to retrieve money from accounts in one country from a point of retrieval in another country
- use of the Hawala banking system, which is largely unregulated and as such allows for anonymous movements of money between jurisdictions
- physical importation of funds in cash or traveller's cheques either by the terrorists themselves on arrival in a country of operation or via couriers
- use of company structures and commercial banking operations to transfer money across borders
- wiring of funds between accomplices in different parts of the world
- use of 'mule accounts' (e.g. students or unemployed persons, or those in debt) where in return for a small payment, the terrorist takes over the use of the account
- either using their own accounts or those of sympathisers.

In a sophisticated financing operation, cash and proceeds from cheques, cash cards, gold, shares, policies, houses, cars, works of art and any number of items representing 'value' are collected into the accounts of charities, high street traders, other legitimate businesses, 'front' companies, 'clean' individuals, mosques, churches, import–export houses, art galleries, etc. ready for onward transmission as invoice payments, investments, contributions, loan repayments, expense reimbursements, intra-entity transfers, salaries and dividend payments, all available for use or further onward movement as and when required. The full range of payment

methods can be deployed from formal wire transfers, money transmission (e.g. Western Union and Moneygram), unofficial money transfer ('hawala' or 'hundi') schemes right through to the withdrawal of cash and its physical transportation via cars, boats, planes, rickshaws, pack animals or people.
Well-organised groups will exploit synergies in the process. For example, throughout the 1980s the LTTE in Sri Lanka (which used to raise an estimated $50 million per annum from various sources) operated a fleet of tankers. The ships not only made profits on legitimate lading contracts, but were also used for smuggling the weapons once they had been purchased and for carrying illegal immigrants to foreign countries as another method of earning money to finance the campaign. Often, business activity and terrorism feed off each other in a mutually dependent relationship. Despite its periodic public slayings of 'drug dealers', the Taliban funded itself from Afghanistan's poppy trade for many years. The Provisional IRA took over and ran profit-making taxi-cab businesses, and bombed Belfast buses and bus stations, ostensibly as part of its campaign of violence, but also to remove the commercial competition. More recently, until it was bombed and fought out of the areas it controlled (a process which, at time of writing in February 2019, seems more or less complete), ISIS was described as 'the richest terrorist organisation in the world' given its operation of its 'Caliphate' as a proto-state:

> **'The Caliphate project, as espoused by its leader Abu Bakr al-Baghdadi, requires, to be viable, infrastructure and superior means to those mustered by Al-Qaeda to carry out its operations. In its - territorial approach (which concerns law, public order, currency, taxes and economic concerns), IS sees itself as a nascent state. It rules over the territory under its control, enacts laws, punishes and rewards, raises taxes and mints currency (the golden dinar). Its publications stress how well its territory is managed, highlighting how well it keeps the peace and how the primary needs of the population are met.'**

(http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/603835/EXPO_IDA(2017)603835_EN.pdf)

Where terror groups such as ISIS actually control territory in this way (as opposed to merely conducting operations within it), a particular problem

arises for agencies and corporations wishing to carry out humanitarian projects or commercial operations there, as illustrated in the following case.

Example

The Lafarge Case

The case of the Swiss building materials conglomerate LafargeHolcim is typical of IS' modus operandi. The factory's management wanted to remain operational despite the seizure of territory by IS, but above all it wanted to ensure the protection of its employees. It obtained the group's permission to pass through checkpoints in exchange for paying taxes. The manufacturer ended up admitting that 'unacceptable' arrangements had been made to protect its cement factory in Jabaliya, 150 kms northeast of Aleppo. Indeed, the company recognised that its local branch belonging to Lafarge 'handed funds over to third parties in order to come to an arrangement with a certain number of armed groups, of which a number were targeted by sanctions', without being able to identify their ultimate recipient. This arrangement also suited the Assad regime – cement is a source of revenue for the Syrian government, which levies taxes on its sale.

Arising out of *'l'affaire Lafarge',* the French government initiated criminal proceedings against the company for terrorist financing and aiding and abetting crimes against humanity, adding to earlier charges which were filed against eight former company executives for financing terrorism and endangering the lives of their Syrian employees.

(https://www.nytimes.com/2018/06/28/business/lafarge-holcim-syria-terrorist-financing.html)

FURTHER DIFFERENCES BETWEEN TERRORIST FINANCING AND CLASSICAL MONEY LAUNDERING

As can be seen from the above, in its deployment of disguising activities to create the appearance of transactional legitimacy, Terrorist Financing (TF) has much in common with its elder sibling, Money Laundering (ML), but there are additional differences.

- *The volume of funds involved.* For serious money launderers handling the proceeds of serious crime, the amounts involved are very large indeed. Current estimates are that there are approximately $1 trillion in criminal assets hiding within the global economy at any given time. That is far more than is likely to be allocated towards the financing of terrorism worldwide. And while many terrorist groups are organised enough to collect very substantial sums running into tens of millions each year, not every attack is spawned from those funds. As the UK's 7/7 bombers showed, a lethal attack on a transport system can be planned and funded well within the confines of an average monthly salary. This poses severe operational difficulties for those organisations (currently primarily banks and other 'gatekeepers' involved in financial services) charged with trying to disrupt the flow of terrorist funds through the financial system. In combating ML, systems are constructed to detect 'suspicious' transactions, where 'suspicious' tends to mean 'unusual', and 'unusual' tends (though not always) to mean 'unusually large'. But as far as the funding of individual attacks is concerned, this approach simply doesn't work. How do you detect an 'unusual' retail purchase or a 'suspicious' mobile phone bill?
- *The status of terrorism (and hence terrorist financing) as a political issue.* Subject to continuing arguments about legal details such as categorisation and mutual enforceability, to a large extent the world now recognises what a criminal is, what criminal money laundering is, and agrees that criminals and money launderers deserve to be caught, punished and stripped of their ill-gotten gains. This is not yet true of terrorism, for the basic reason that there is still no full

international agreement on what a ‘terrorist’ actually is and on what constitutes ‘terrorism’. While very few will promote or defend the concept of deliberately causing civilian deaths as a legitimate means of pursuing a cause, the old axiom that ‘one man’s terrorist is another man’s freedom fighter’ still applies. Consequently, terrorist financing as an issue has a political ‘edge’ to it that money laundering does not. It makes it a much more sensitive and complicated issue for organisations and governments to deal with, especially in light of the invidious ways in which, in free societies, terrorist groups operate within what we may call innocent society.

■ *The extension of terrorist financing into innocent society.* Non-terrorist criminals and terrorists tend to treat innocent society very differently. If you are not actually a criminal, if you do not live a ‘criminal lifestyle’ (basically spending lots of cash whose origins you can’t explain) and if you do not consort with criminals or seek their company, then other than through mistaken identity, you are unlikely to be thought of as a criminal by society at large. Moreover, other than in your designated role as victim, criminals themselves will most likely leave you alone. As a stranger, they are unlikely to try to recruit you to their cause, ask you to drive their getaway car, or request the use of your bank account to collect their cash before wiring it to an offshore haven. Not for nothing is it called ‘the underworld’ – a phrase aptly denoting the parallel yet separate existence of the criminal community.
The same isn’t true of terrorist financing. As has been described, serious terrorist groups committed to long-term operations will finance their activities using any means they can, and the national, ethnic or religious groups from which they are drawn – be they minority communities within specific countries or diaspora spread around the world – will often pay a heavy price for ‘the cause’. Many who detest the terrorists’ methods will still be viewed with suspicion and fear by wider society. Those who try to disassociate themselves and their families from any connection with terrorism often face pressure to support, to assist or to ‘get involved’ in some way, shape or form, with punishment or ‘discipline’, often invisible to the rest of society, being meted out to those who refuse to conform. And even when they seek to give charity for the support of their own community, whether at home

or overseas, they risk the conversion of that most humane of acts into murderous purposes.

SUSPICION RECOGNITION

A critical requirement of financial institutions and others charged with responsibilities for the detection and prevention of ML and TF is that they report instances when they suspect that their facilities and services may have been used by their customers and clients for criminal purposes. But when should you be suspicious? We deal with this key question later in more detail, but for now let's track the process of how suspicion might develop in a fairly typical, potential money laundering scenario using the example of the Pecunia Banking Corporation. In this fictitious example we will consider at each stage, and *purely on the information presented*, whether or not we are either 'neutral', 'uncomfortable' or 'suspicious' about this client.

Example

Pecunia Banking Corporation

Stage 1

You are newly employed by AlnaBank Global and are reviewing existing relationships. The client you are looking at this morning is Pecunia - Banking Corporation (PBC) which has a correspondent banking relationship with Alna. PBC is a registered Russian bank with, the file states, a number of important corporate clients and its stated purpose in wanting to set up a correspondent relationship is to be able to service its clients' needs in Europe.

PBC's reason for wanting a correspondent relationship seems perfectly reasonable. There are no particular issues here. The bank is a Russian bank, and everyone knows that Russian banks have been exploited in the past by those wishing to move illicit wealth from the country, but there is nothing on these facts which stands out in that regard.

Stage 2

PBC was incorporated in 2009 and has a registered head office at 23 - Sevatskaya Street, Moscow, which a map reveals is in a suburb. A certified copy of PBC's Certificate of Incorporation has been examined and is authentic. PBC's appointed representative is Mr Ginatulin, the Managing Director to whom AlnaBank staff speak to on a weekly basis. A copy of his identification is on the file.

A number of questions are now starting to emerge as we find out more about PBC. The bank is clearly not well established, as it has only existed since 2009. The bank's registered office is not in central Moscow, but rather in a distant suburb. What and where is Sevatskaya Street? Is it possible that the bank might be a 'shell bank', i.e. a bank that does not have a genuine physical presence in the country where it is incorporated?

Stage 3

Mr Ginatulin is on PBC's Board of Directors. Mr Shimanenko is the only other named Director, and his identification details are also on the file. There are ten shareholders, each owning between 5 per cent and 15 per cent of PBC. All the shareholders are corporate entities (e.g. Infolink, Poldavic Professional Services). All except one are subsidiaries of a company called 'International Distributions'.

PBC's ownership is, effectively, shrouded in mystery because we do not know who exactly controls it. There are two named directors, but they are

not shareholders. The shareholders are all corporate entities, and these are almost all owned in turn by another corporate entity called ‘International - Distributions’. Who owns these businesses? Who are the individual people behind these company names? The extent to which this bank appears to want to hide its ownership is potentially very suspicious indeed.

Stage 4

Your bank has clearly asked Mr Ginatulin about PBC’s client base and the nature of its business. Mr Ginatulin has stated that it acts for a number of well-known Russian companies, some of whom are involved in the film industry. There are photocopies of letters of instruction from some of these companies. Mr Ginatulin has also referred staff to PBC’s website, where there are pages about the bank’s products and services. There are multiple references to the management team, but no other bank managers or employees are identified or named anywhere on the website.

AlnaBank is really none the wiser about what PBC and its clients really do. The client letters are photocopies not originals so they could be forgeries and ‘being involved in the film industry’ isn’t really a sufficient description of the type of business. Shell banks might attempt to give themselves a legitimate presence by setting up websites and putting out information to give the impression of normal banking business. In this particular instance there is some information about products and services but *still* no information about the bank’s history or its ownership.

Stage 5

Transaction records show very large volumes of funds being put through the account over the two years during which it has been open – nearly $1 billion. Many of the transactions are stated to be on account of well-known Russian companies, with monies being received and then forwarded on to

other banks in the US, but about half – some $400 million – is stated to be on account of ‘International Film Distributions’ for purchasing film rights. These payments have been made to Hollywood Bank in the Bahamas, which appears to be a genuine bank.

There is a disturbing lack of any independent verification of any of the information provided. One billion dollars is a very large sum for through-put within two years, so you had better be sure that the business is genuine. It is also particularly noteworthy that funds have been sent to the US and the Bahamas, whereas the business purpose stated on the file was to service clients’ European needs. No information is given on the value of the film rights purchased. If the purchase related to the *Lord of the Rings* franchise, then maybe the payment would be justified. But the purchase of valueless offshore assets from associates in order to suppress profits is a well-known tax evasion strategy, and by now it is indeed starting to look as if that may be what is going on here.

In short, this is a relationship about which there is a chronic shortage of information. While technical requirements such as identification and certification documents litter the file, along with ‘famous name’ clients, we do not really know whether the bank has a physical existence, who ultimately controls it, whether its clients are genuine, what business they are engaged in, and how and why they are making their payments. Definitely suspicious!

2

The International AML and CFT Framework

Key components of the international institutional and legal framework

A developing framework to combat tax evasion

Proliferation financing

A developing framework for the regulation of cryptocurrencies

The Financial Action Task Force (FATF)

FATF regional style bodies and associate members

Other relevant international bodies

KEY COMPONENTS OF THE INTERNATIONAL INSTITUTIONAL AND LEGAL FRAMEWORK

The best and easiest way to view the international framework for combating money laundering and terrorist financing, is as a scale of activity, ranging from the international, to the regional, to the national, to the institutional and finally to the individual level. The framework is shown in Figure 2.1, with slight variations for each jurisdiction.

UN conventions and resolutions

UN Single Convention on Narcotic Drugs 1961; UN Convention on Psychotropic Substances 1971; UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988 (the Vienna Convention)

Collectively, these conventions have provided the international legal framework for the 'war on drugs', i.e. the global control and scheduling of various categories of drugs deemed harmful or abusive, including opium, heroin, cocaine, cannabis, ecstasy and LSD to name but a few.

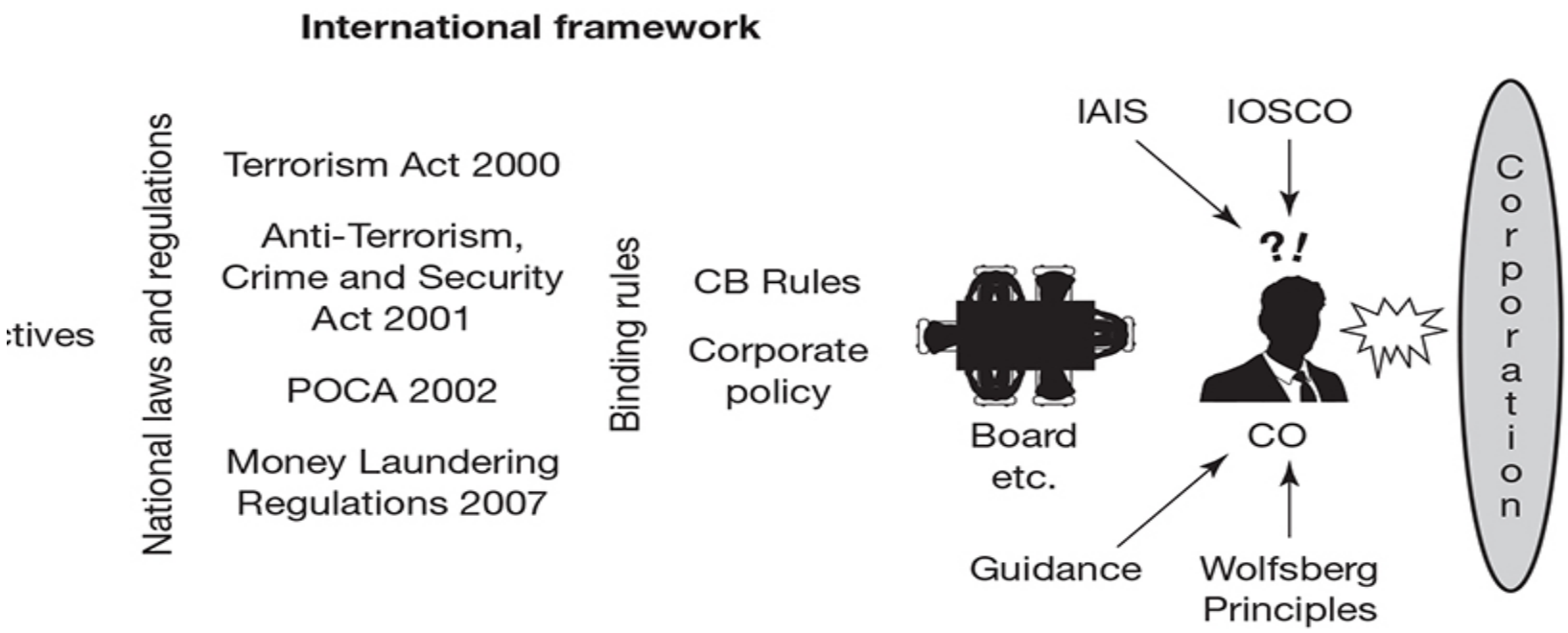
The 1988 Convention agreed in Vienna went further. Its Article 5 (Confiscation) required states to cooperate in various ways in seizing and confiscating the proceeds of trafficking in illegal narcotics. Its particular focus was on mutual legal cooperation in such areas as extradition, search and seizure, service of documents, the transfer of legal proceedings between

jurisdictions and preventing bank secrecy laws being used to prevent the mutual transfer of information relevant to a case.
Crucially, Article 3 (Offences and Sanctions) also required states to criminalise the laundering of the proceeds of illegal narcotics trafficking through the financial system, thus paving the way for the setting up of the international anti-money laundering (AML) system.

UN Convention for the Suppression of the Financing of Terrorism 1999

The UN has had an anti-terrorist financing regime in place for some time on state actors (the so-called 'rogue states', such as Libya and Iran). It was only in the second half of the 1990s that the financing of terrorism by non-state actors came to the fore.
Following a series of resolutions condemning terrorist action during the 1990s, the UN adopted this convention at the General Assembly held in New York in December 1999. The resultant treaty came into force in April 2002. Article 2 of the Convention requires countries to criminalise the act of providing or collecting funds with the intention or knowledge that those funds will be used to carry out a terrorist attack. The Convention asserts that 'financing is at the heart of terrorist activity' and lays out the foundations for closer cooperation between law enforcement agencies, financial authorities and individual countries.

Figure 2.1 The international AML CFT legal framework (as seen from a UK legislative perspective)


International framework
tives
National laws and regulations
Terrorism Act 2000
Anti-Terrorism, Crime and Security Act 2001
POCA 2002
Money Laundering Regulations 2007
Binding rules
CB Rules
Corporate policy
IAIS
IOSCO
?!
Board etc.
CO
Guidance
Wolfsberg Principles
Corporation

Countries that have ratified the treaty (known as State Parties) are required to put into place mechanisms to identify, detect and freeze or seize assets used or earmarked for terrorist activities, and financial institutions are called upon to be vigilant with regard to unusual transactions and to report to the authorities anything that they suspect may have links with terrorism or terrorist activities. They are also obliged to prosecute or extradite offenders, and to cooperate with other countries' investigations. A State Party cannot, for example, turn down a request for mutual legal assistance on the grounds of its own banking secrecy laws.

UN Security Council Resolution 1373 2001

Following the attacks on the World Trade Center in September 2001, the United Nations Security Council passed UNSCR 1373 for the Suppression of the Financing of Terrorism. This is one of the lynchpins of international action against terrorist financing, and includes a range of steps and strategies to combat the financing of terrorism generally.

Resolution 1373 builds on the UN blacklisting regime which started with the creation of the Al-Qaeda and Taliban lists with UN Security Council Resolution 1267, following the 1998 Al-Qaeda attacks on the US embassies in Kenya and Tanzania. Resolution 1267 called upon all states to freeze funds and other property that may be used directly or indirectly to benefit the Taliban. Created in the aftermath of 9/11, Resolution 1373 goes a few steps further and encourages states to create their own blacklists.

Resolution 1373 reconfirms that all states should prevent or suppress terrorist financing, criminalise fundraising or the provision of economic resources for terrorism, and freeze the financial assets of terrorist groups. Terrorist acts should be established as serious criminal offences and anyone involved in their financing, planning or perpetration should be denied any kind of support and brought to justice. Particular emphasis is placed on the exchange of information between countries, not only with regard to terrorist actions and movements but also in light of the close links between terrorist acts and other types of organised crime and money laundering.
Critically, UNSCR 1373 continued the extension of the existing notification and sanctions regime, already applicable to 'rogue states', to individuals and organisations suspected of connections with terrorism. This led to the establishment of an international blacklist of suspected terrorists. Resolution 1373 also established the Counter-Terrorism Committee (CTC) as a monitoring body to try to ensure the Resolution is effectively implemented and to provide assistance for countries that need help in this regard.

UNSCR 1624 2005

The UN's 50-year anniversary in September 2005 saw the adoption of UNSCR 1624, which among other things stresses that countries should criminalise *incitement* to commit terrorist acts and calls upon states to strengthen international border security. This development was a direct response to the open preaching of overtly violent and/or aggressive messages by, in particular, a small minority of Muslim clerics.

European Union Directives and Council Common Positions

European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime 1990 (The Strasbourg Convention)

This was signed in Strasbourg in 1990 and entered into force in September 1993. The Convention aimed to counter laundering of the proceeds of *all* types of crime (not just drug trafficking) and to improve international cooperation (Chapter III of the Convention), both between Council of Europe member states and with other countries around the world. With

specific reference to money laundering the Convention included provisions for the establishment of a range of laundering offences (Chapter II Article 6). It also included provisions for the confiscation of the proceeds of crime and for ordering the disclosure of bank, financial and commercial records to facilitate the tracing and identification of such proceeds (Chapter II, Articles 2 and 4).

European Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, and on the Financing of Terrorism 2005 (Convention # 198)

Updating and expanding on the 1993 Convention agreed in Strasbourg, this more recent Convention was adopted by the Committee of Ministers in May 2005 and is firmly grounded in the 1999 UN International Convention for the Suppression of the Financing of Terrorism (discussed above). Crucially, in Chapter II Article 2(2) the Convention focuses not only on the laundering and confiscation of criminal proceeds, but also on the interdiction of 'clean' money generated through legitimate sources but destined for criminal purposes – a key activity for financiers of terrorism, as has been noted. The text addresses the fact that quick access to financial information or information on assets held by criminal organisations, including terrorist groups, is key to the successful implementation of preventive and suppressive measures against them.

EU Money Laundering Directives

There have been five EU Directives dealing with Money Laundering.
The First Directive, in 1991 was the 'basic package' and required member states to implement laws centred around the Financial Action Task Force 40 – FATF 40 (see later in this chapter). It applied, however, only to a restricted range of financial institutions and only to the proceeds of drug related crimes. Accordingly, the Second Directive of 2001 extended both the range of crimes to be covered under national legislation and regulation, and also the categories of institutions to be affected, extending the latter to include not just banks but also 'gatekeepers' such as lawyers, notaries, trust or company service providers, accountants, auditors, tax advisers, real estate agents, casinos, auctioneers and other dealers in high-value goods.
The Financial Action Task Force's previous review of its 40 Recommendations in 2003, together with the addition of nine Special

Recommendations and other associated international activity in relation to terrorist financing resulted in the creation of a Third EU Directive of October 2005 (which came into force in the member states on 15 December 2007).
The Third Directive explicitly addressed terrorist financing as well as money laundering. It also contained more detailed 'customer due diligence' provisions than previous Directives. In particular these:

- were defined as comprising not just customer identification and verification of identity, but also establishment of the purpose and intended nature of the business relationship and ongoing monitoring
- applied to new and existing customers
- required identification of beneficial owners and the verification of the beneficial owner's identity
- introduced exemptions from full customer due diligence ('simplified due diligence') for certain low-risk situations, and
- required 'enhanced due diligence' measures for situations that - present a higher money laundering or terrorist financing risk, at least for non-face-to-face business, 'politically exposed persons' and international correspondent banking relationships.

Furthermore:

- The Directive provided for comitology measures – legally binding implementing measures the Commission could adopt to clarify certain provisions of the Directive. Among others, the Commission may adopt criteria for simplified and enhanced due diligence, definitions of, for example, beneficial owner and politically exposed persons, and identify third countries that do not meet the provisions of the Directive.
- It recognised in EC law the concept of a risk-based approach to anti-money laundering.
- It applied a licensing/registration system for 'currency exchange offices', trust and company service providers involving a 'fit and proper' test for those who directly or beneficially owned such businesses.
- It required financial firms to apply customer due diligence and - record-keeping standards to overseas branches and majority-owned -

subsidiaries (unless not permitted by local law).

- It introduced more explicit obligations on institutions to have systems for AML risk management and compliance.
- It included miscellaneous provisions on, for example, the suspicious activity reporting regime and the relationship with financial intelligence units.

A key feature of the Fourth Directive, which came into force on 26 June 2017, was its much-increased emphasis on the use of risk-based approaches at every level. The Third Directive gave legal recognition to the concept of a risk-based approach. The Fourth Directive went further, with requirements for:

- EU states to commission national assessments of money laundering and terrorist financing risks
- individual institutions to develop risk-based policies, procedures and controls
- individuals working in these institutions to conduct risk-based CDD for all their business.

Counting the number of times the word ‘risk’ appears in consecutive Directives gives some indication of the increasing importance that has been attached to risk-based approaches. The Third Directive mentioned ‘risk’ just 13 times, whereas the Fourth Directive mentions it at least 149 times.
The Fourth Directive introduced other significant changes:

- a lower maximum threshold (Eur 7,500) and tighter record-keeping requirements for cash transactions
- a tightening up of the enhanced due diligence measures for Politically Exposed Persons
- a requirement for firms to maintain accurate, up-to-date records regarding the beneficial ownership of assets and for this information to be provided to government and held in a central register from where it could be shared with relevant authorised parties including other firms
- a requirement that EU firms with majority-owned subsidiaries in countries with less strict regimes must comply in those countries with the stricter provisions of their EU home country.

The Fourth Directive also included an amendment to the rules for Simplified Due Diligence (SDD) that had been introduced under the Third Directive. Under the Third Directive, firms were able automatically to apply SDD to certain types of legal person, for example:

- firms subject to regulation under the EU AML Directives or equivalent legislation
- companies whose securities are listed on a regulated market
- public authorities.

Under the Fourth Directive firms could no longer automatically default to SDD in any circumstance and may only use SDD following an evidence-based risk assessment of the individual or entity in question.

On 19 June 2018 the EU published a Fifth Money Laundering Directive. The Fifth Directive constitutes part of the EU's Action Plan against terrorism which was announced in February following terrorist attacks in Paris and Brussels and in response to the publication of the Panama Papers in April 2016. Hot on the heels of the Fourth Directive which had come into force just one year previously, the Fifth Directive is not as extensive as its precedent, although it does contain some important new provisions.

Under the Fifth Directive the scope of the regulatory regime has been extended to include virtual currency exchange platforms and customer wallet providers. Other provisions include:

- making information about the beneficial ownership of EU-based companies available to members of the general public
- requiring firms to consult the beneficial ownership register as part of their due diligence activity
- requiring EU member states to create a list of the national public offices and functions that qualify as having a PEP status
- robust enhanced due diligence measures for financial flows emanating from high-risk countries
- prohibiting anonymous bank accounts and safe deposit boxes
- making real estate ownership information centrally available to public authorities
- lowering the thresholds at which the purchasers of prepaid cards and users of e-money must be identified

- strengthening the powers of Financial Intelligence Units (FIUs) and enhancing the arrangements for cooperation and information exchange between relevant authorities.

Council Common Position (2001/931/CFSP)

December 2001 also saw the implementation of a Council Common Position in drawing up a list (since regularly updated) of individuals, groups and entities involved in terrorism whose assets were to be frozen. The list at that time included ETA (Basque Fatherland and Liberty), the IRA (Irish Republican Army), GRAPO (the First of October Anti-Fascist Resistance Group), the terrorist wing of HAMAS, Palestinian Islamic Jihad and other revolutionary activist groups, as well as the names of individuals belonging to such groups.
Since 2001 the list has been updated on a six-monthly basis. At the time of publishing the latest update, (CFSP) 2019/25 of 8 January 2019, identified the following individuals, groups and entities:

I. Persons

1. ABDOLLAHI Hamed (a.k.a. Mustafa Abdullahi), born 11.8.1960 in Iran. Passport number: D9004878.
2. AL-NASSER, Abdelkarim Hussein Mohamed, born in Al Ihsa (Saudi Arabia), citizen of Saudi Arabia.
3. AL YACOUB, Ibrahim Salih Mohammed, born 16.10.1966 in Tarut (Saudi Arabia), citizen of Saudi Arabia.
4. ARBABSIAR Manssor (a.k.a. Mansour Arbabsiar), born 6.3.1955 or 15.3.1955 in Iran. Iranian and US national. Passport number: C2002515 (Iran); Passport number: 477845448 (USA). National ID no.: 07442833, expiry date 15.3.2016 (USA driving licence).
5. ASADI Assadollah, born 22.12.1971 in Teheran (Iran), Iranian national. Iranian diplomatic passport number: D9016657.
6. BOUYERI, Mohammed (a.k.a. Abu ZUBAIR, a.k.a. SOBIAR, a.k.a. Abu ZOUBAIR), born 8.3.1978 in Amsterdam (The Netherlands).
7. EL HAJJ, Hassan Hassan, born 22.3.1988 in Zaghdraiya, Sidon, Lebanon, Canadian citizen. Passport number: JX446643 (Canada).
8. HASHEMI MOGHADAM Saeid, born 6.8.1962 in Teheran (Iran), Iranian national. Passport number: D9016290, valid until 4.2.2019.

9. IZZ-AL-DIN, Hasan (a.k.a. GARBAYA, Ahmed, a.k.a. SA-ID, a.k.a. SALWWAN, Samir), Lebanon, born in 1963 in Lebanon, citizen of Lebanon.
10. MELIAD, Farah, born 5.11.1980 in Sydney (Australia), Australian citizen. Passport number: M2719127 (Australia).
11. MOHAMMED, Khalid Shaikh (a.k.a. ALI, Salem, a.k.a. BIN KHALID, Fahd Bin Adballah, a.k.a. HENIN, Ashraf Refaat Nabith, a.k.a. WADOOD, Khalid Abdul), born 14.4.1965 or 1.3.1964 in Pakistan, passport number 488555.
12. S,ANLI, Dalokay (a.k.a. Sinan), born 13.10.1976 in Pülümür (Turkey).
13. SHAHLAI Abdul Reza (a.k.a. Abdol Reza Shala'i, a.k.a. Abd-al Reza Shalai, a.k.a. Abdorreza Shahlai, a.k.a. Abdolreza Shahla'i, a.k.a. Abdul-Reza Shahlaee, a.k.a. Hajj Yusef, a.k.a. Haji Yusif, a.k.a. Hajji Yasir, a.k.a. Hajji Yusif, a.k.a. Yusuf Abu-al-Karkh), born circa 1957 in Iran. Addresses: (1) Kermanshah, Iran, (2) Mehran Military Base, Ilam Province, Iran.
14. SHAKURI Ali Gholam, born circa 1965 in Tehran, Iran.
15. SOLEIMANI Qasem (a.k.a. Ghasem Soleymani, a.k.a. Qasmi Sulayman, a.k.a. Qasem Soleymani, a.k.a. Qasem Solaimani, a.k.a. Qasem Salimani, a.k.a. Qasem Solemani, a.k.a. Qasem Sulaimani, a.k.a. Qasem Sulemani), born 11.3.1957 in Iran. Iranian national. Passport number: 008827 (Iran Diplomatic), issued 1999. Title: Major General.

II. Groups and entities

1. 'Abu Nidal Organisation' – 'ANO' (a.k.a. 'Fatah Revolutionary - Council', a.k.a. 'Arab Revolutionary Brigades', a.k.a. 'Black - September', a.k.a. 'Revolutionary Organisation of Socialist Muslims').
2. 'Al-Aqsa Martyrs' Brigade'.
3. 'Al-Aqsa e.V'.
4. 'Babbar Khalsa'.
5. 'Communist Party of the Philippines', including 'New People's Army' – 'NPA', Philippines.
6. 'Directorate for Internal Security of the Iranian Ministry for - Intelligence and Security'.
7. 'Gama'a al-Islamiyya' (a.k.a. 'Al-Gama'a al-Islamiyya') ('Islamic Group' – 'IG').

8. ‘·Islami Büyük Dog˘u Akıncılar Cephesi’ – ‘IBDA-C’ (‘Great Islamic Eastern Warriors Front’).
9. ‘Hamas’, including ‘Hamas-Izz al-Din al-Qassem’.
10. ‘Hizballah Military Wing’ (a.k.a. ‘Hezbollah Military Wing’, a.k.a. ‘Hizbullah Military Wing’, a.k.a. ‘Hizbollah Military Wing’, a.k.a. ‘Hezballah Military Wing’, a.k.a. ‘Hisbollah Military Wing’, a.k.a. ‘Hizbu’llah Military Wing’, a.k.a. ‘Hizb Allah Military Wing’, a.k.a. ‘Jihad Council’ (and all units reporting to it, including the External Security Organisation)).
11. ‘Hizbul Mujahideen’ – ‘HM’.
12. ‘Khalistan Zindabad Force’ – ‘KZF’.
13. ‘Kurdistan Workers’ Party’ – ‘PKK’, (a.k.a. ‘KADEK’, a.k.a. ‘KONGRA-GEL’).
14. ‘Liberation Tigers of Tamil Eelam’ – ‘LTTE’.
15. ‘Ejército de Liberación Nacional’ (‘National Liberation Army’).
16. ‘Palestinian Islamic Jihad’ – ‘PIJ’.
17. ‘Popular Front for the Liberation of Palestine’ – ‘PFLP’.
18. ‘Popular Front for the Liberation of Palestine – General Command’ (a.k.a. ‘PFLP – General Command’).
19. ‘Devrimci Halk Kurtulus, Partisi-Cephesi’ – ‘DHKP/C’ (a.k.a. ‘Devrimci Sol’ (‘Revolutionary Left’), a.k.a. ‘Dev Sol’) (‘Revolutionary People’s Liberation Army/Front/Party’).
20. ‘Sendero Luminoso’ – ‘SL’ (‘Shining Path’).
21. ‘Teyrbazen Azadiya Kurdistan’ – ‘TAK’ (a.k.a. ‘Kurdistan Freedom Falcons’, a.k.a. ‘Kurdistan Freedom Hawks’).

Source: © European Union, http://eur-lex.europa.eu/

EU Markets in Financial Instruments Directive (Mifid I and II)

The Markets in Financial Instruments Directive (Mifid) was introduced by the EU in 2007. The legislation introduced tighter regulation around firms that trade in and provide client services related to financial instruments such as shares, bonds, unit trusts and derivatives. It also regulated the venues where trading in such financial instruments was carried out. It was designed to increase transparency in the equities markets and, through the introduction of a Multilateral Trading Facility (MTF), to open up the competition between trading venues. Its impact on the equities markets was substantial, with effects including a general lowering of transaction costs

and faster trading times. But the legislation had its downsides too. The increased number of trading venues caused fragmentation in the EU equities market and led also to an increase in dark trading.
Mifid II took seven years to pull together and came into force on 3 January 2018. Its overall intention is to reinforce protection afforded to investors and to increase investor confidence. It aims to ensure that the European financial markets are a safer, more transparent and more efficient place for investors to do business. In the pursuit of these aims Mifid II is designed to extend the beneficial effects of Mifid and at the same time to address some of its more negative effects including the increase in dark trading. It is also designed to address new risks that have arisen through technological developments and the new methods that have emerged as a result, such as high-frequency algorithmic trading.
Key effects of Mifid II include:

- reduced OTC (over-the-counter) trading and increased trading through regulated trading venues
- an extension of the transparency regime to cover a much wider range of financial instruments (the markets covered under Mifid II include the equities, fixed income, commodities, currencies and futures markets and also exchange-traded products and retail derivatives)
- the promotion of more orderly markets via new rules and provisions for algorithmic and high-frequency algorithmic trading
- the promotion of increased competition in trading and clearing markets.

Mifid II introduces substantial new disclosure and reporting requirements that have required the review and realignment of firms' systems. Under the new regime firms are required to disclose post-trade information on a much wider range of financial instruments as close to real time as possible. Firms are also required to expand the range of data about transactions that is collected and reported to competent authorities. There are more stringent requirements for trading that involve high-frequency algorithmic trading techniques, and also for operators of trading venues.

Important US and UK legislation

The international legal framework that we have outlined here sets clear parameters for legislation and regulation at the national level. While it is not feasible for the purposes of this book to conduct a complete analysis of *all* countries' provisions we have, nonetheless, summarised below some key aspects of both US and UK legislation, both major jurisdictions with very large financial sectors that have a bearing on the AML and CFT activities of financial firms worldwide.

US Patriot Act 2001

The Patriot Act is US legislation and clearly country-specific, but it was a seminal response to the 9/11 terror attacks and had a substantial impact on AML and CFT legislation across the globe. Passed in the aftermath of the attacks, this wide-ranging piece of legislation promulgated stiff provisions affecting all financial firms with business touching the US directly or indirectly. In short, the Act is significant because its ramifications extend well beyond US territory and beyond US institutions. It also sets in place a number of counter-terrorist financing measures that have since become adopted as part of the international standard for best practice in combating terrorist financing.

Title III (International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001) prohibits 'covered financial institutions' (basically US banks and US branches of non-US banks) from opening correspondent accounts with foreign shell banks (i.e. banks which did not have a physical presence in the jurisdiction where they were incorporated and which were not part of a larger group), and from doing business with other banks which *did* have relationships with foreign shell banks. It imposed enhanced due diligence requirements in respect of correspondent and private banking relationships with foreign banks (requirements again applying to both US banks and the US branches of foreign banks) and asserted 'long arm' jurisdiction over the assets of foreign money launderers, in so far as their accounts, assets or transactions touched the US.

US Final Rule on Customer Due Diligence

A more recent development in the US's anti-money laundering provision has been the introduction of the Final Rule on Customer Due Diligence. The Final Rule refers to new FinCen rules which came into force on 11 May 2018. In brief, the Rule requires financial institutions to collect,

maintain and report details of beneficial ownership for any accounts or assets it holds.
The Rule is part of a general movement by the US government to modify legislation and tighten up the provisions that it has in place to combat money laundering and terrorist financing. The Patriot Act modified the Bank Secrecy Act, enabling the US Treasury to require financial institutions to record and file reports as appropriate on their customers' activities. The release of the Panama Papers in 2016 and more recently the Paradise Papers in 2018 has clearly demonstrated that existing identification and record-keeping provisions have not been able to prevent the wide-ranging use of offshore accounts, complex structures, shell companies, nominees, trusts and other methods to disguise beneficial ownership in order to launder funds.
The Final Rule is designed to close loopholes and to ensure as far as possible that beneficial ownership cannot be hidden.

UK Criminal Finances Act 2017

The UK Criminal Finances Act came into force on 30 September 2017. The Act marked a significant move forward in the fight against money laundering with key developments including:

- the creation of Unexplained Wealth Orders, or UWOs
- new provisions to allow information sharing between regulated companies in relation to suspicions of money laundering or terrorist financing.

The Act also introduced a new corporate offence of failing to prevent the facilitation of tax evasion, which is discussed later in this chapter, in relation to other tax evasion legislation.

Unexplained Wealth Orders

Unexplained Wealth Orders (UWOs) were introduced into the UK under the Criminal Finances Act 2017. They are an emerging tool that can significantly strengthen the authorities' hand in the fight against money laundering. Countries other than the UK that have adopted UWOs (or some version thereof) include Australia, Colombia, Ireland, South Africa, New Zealand, France and some provinces in Canada.

UWOs address a specific legislative difficulty, which is the ability for authorities to freeze or recover suspicious funds without a pre-existing conviction against the owner or the property in question. Criminals go to great lengths to disguise the origins of their funds. It's not always possible to prove beyond doubt that certain funds are the proceeds of crime. Even where a conviction exists it may not always be possible to link suspicious assets to the unlawful activities for which the person was convicted. This means that, even if law enforcement agencies have strong grounds to *believe* that assets were acquired using unlawful funds, then without proof there may be little they can do about it.

UWOs turn this problem on its head, because they put the onus of proof on the owner of the asset. Although the specifics of the legislation may vary across the countries that use UWOs, the basic principle remains the same: if an individual has assets whose value appears disproportionate to their known income then a UWO can require them to explain the origin of those assets and to provide tangible evidence of their legitimacy; if they are unable to do this, then the assets may be seized.

UWOs do not rely on a successful prosecution and conviction for assets to be seized. In effect this makes it easier for UK agencies to seize assets that have even a taint of illegitimacy about them. This in turn means that seizure actions arising from UWOs are potentially far more likely and the odds somewhat shortened that a firm will, at some stage, find itself associated with a client who has been the subject of a seizure. Where a client becomes the subject of a UWO then that could raise questions about the quality and robustness of an institution's procedures for verifying their clients' sources of wealth. The use of enforcement instruments such as UWOs therefore places additional scrutiny on financial firms and their conduct in relation to:

- accurately identifying and verifying their clients' wealth and sources of income
- identifying and reporting apparent inconsistencies between their clients' apparent assets and known wealth.

Information Sharing Provisions

The Criminal Finances Act also introduced new provisions to allow banks and other businesses in the regulated sector to share information on a voluntary basis where there is a suspicion that a person or entity may be

engaged in money laundering or terrorist financing activities. Under the provisions, the information sharing may be instigated by a regulated firm itself. The information sharing is entirely voluntary and regulated firms can refuse to take part. The aim is to strengthen existing suspicion reporting provisions by enabling firms to alert each other to possible suspicious activity in a way that they were previously unable to do and, in so doing, to assist firms in their collective effort to identify and combat financial crime.
This voluntary information sharing is separate from existing requirements to file suspicious activity reports (SARs) with the authorities. SARs remain mandatory and, assuming that a firm has suspicions that it wants to share with another firm, then this information sharing needs to be carried out in tandem with existing obligations to file an SAR of their suspicions.

The Interaction between AML and CFT Legislation and Privacy Considerations

Two of the fundamental requirements of all AML and CFT legislation are that firms must:

- verify their clients' identity, their sources of wealth and link them to any assets where they have a beneficial ownership interest
- disclose relevant information about their clients to the relevant authorities, in the event of a suspicion.

Balanced against this, firms also have legal duties and obligations relating to their clients' privacy rights. Firms are required to protect the confidentiality and integrity of client records. Diligence in safeguarding their clients' privacy is an essential part of their duty to keep clients safe and to protect them from identity theft, fraud and other risks.
On the face of it these two sets of legal obligations are set against one another. On the one hand, privacy laws (e.g. such as those required by the EU General Data Protection Regulation (GDPR) which came into force on 28 May 2018) state that personal data must not be disclosed without the person's knowledge or consent. On the other, AML and CFT laws require that firms *do* disclose the details of people who are the subject of a suspicion – and moreover they are specifically prohibited from seeking their consent or otherwise letting them know, i.e. tipping off.

Of course different countries' laws are not all entirely the same and firms need to take care to ensure that compliance with one law does not place them in breach of another. Generally privacy laws *do*, however, allow for the disclosure of information without a person's consent in certain circumstances, including where there is a legal requirement under separate legislation to make the disclosure.

In short, firms *do* have an obligation to protect the confidentiality of their clients' information, but only insofar as it does not conflict with their obligation to disclose suspected wrongdoing on the part of their client. Privacy rights are rarely if ever absolute and are subject to condition. An individual's suspected or known involvement in criminal activity will almost always override their right to privacy, and a firm will normally be able legally to disclose information relevant to that suspected activity *without* falling foul of privacy laws, if they have operated their procedures correctly.

A DEVELOPING FRAMEWORK TO COMBAT TAX EVASION

Tax evasion usually involves the concealment of *legally* obtained funds in order to avoid paying the taxes due. Tax evasion poses a serious threat to government revenues worldwide, and particularly since the start of the global economic crisis in 2008 there have been significant developments in the international cooperative effort to combat tax evasion.

The Organization for Economic Co-operation and Development (OECD) has long been engaged in facilitating cooperation across jurisdictions in the fight against tax evasion. The OECD's Global Forum on Transparency and Exchange of Information for Tax Purposes is a multilateral framework which seeks to implement and monitor the implementation of standards of transparency and exchange of information for tax purposes. The OECD standards provide for the international exchange on request of foreseeably relevant information for the administration or enforcement of the domestic tax laws of a requesting party.

With its Foreign Account Tax Compliance Act (FATCA), enacted in 2010, the US has been aggressive in introducing harsher national measures designed to reinforce internationally agreed standards by legislating to *enforce* the disclosure of US taxable income held outside the US, to place obligations on both taxpayers and the foreign financial institutions holding their assets and to penalise those taxpayers and institutions that do not cooperate or make accurate information about their US-based income available.

Under FATCA, US persons and entities holding financial assets outside the US are expected to report those assets to the US Internal Revenue Service (IRS). Foreign financial institutions – or FFIs – are also required to report to the IRS on financial accounts held with them by US persons and entities, or by foreign entities in which US persons have a significant (10 per cent or more) ownership interest. FFIs need to enter into an agreement with the IRS to comply with FATCA, or otherwise do no further business with US clients or US securities. If an FFI has not entered into such an agreement but nonetheless continues to do business with US entities and securities then it becomes subject to a fairly punitive withholding tax on all its US-based income. In other words, any FFI wishing to do US business really has very little option *but* to comply with FATCA. Compliance with FATCA also requires FFIs to carry out specific due diligence in order to identify their US clients; and to withhold and/or deduct a withholding tax on the US-based income of any US clients who themselves have not complied with their obligations under FATCA. With the due diligence requirements of this law there are some obvious parallels with the anti-money laundering and counter-terrorist financing procedures and systems already used by affected financial institutions.

The introduction of FATCA has had implications in that financial institutions have needed to review and update their existing provisions for account opening, account monitoring, record-keeping and reporting in order to ensure compliance and avoid becoming subject to a withholding tax.

At the time that FATCA was being introduced there was a high expectation that other legislation would soon follow to facilitate greater transparency and sharing of tax information between jurisdictions. As stated above, the OECD had long been working towards a framework for international co-operation in combating tax evasion. Moving with the impetus created by FATCA, the OECD got together in 2014 with G20 countries, the EU and

other international bodies to develop a Standard for Automatic Exchange of Financial Account Information in Tax Matters. Known more generally as the Common Reporting Standard, the idea is to equip tax authorities with the tools and powers they need to access information about their residents' overseas assets and to combat offshore tax evasion. The Common Reporting Standard builds on the systems and controls for cross-border sharing of tax information that had already been developed for FATCA.
One way of looking at the Common Reporting Standard is that it is part of a global, intergovernmental effort to make tax evasion much more difficult. The basics are as follows:

- customers wishing to do business with a financial institution are required to provide identification including information about the nationality of beneficial owners and controlling persons
- the financial institution collects this information and links it to the assets held
- the financial institution then reports this information to the local tax authority
- the local tax authority then exchanges the information with foreign tax authorities in the jurisdictions of the beneficial owners and controlling persons.

By 29 May 2019, over 100 jurisdictions had committed to the automatic exchange of tax information.
A more recent development has been the enactment of laws that make individual firms accountable for the actions of their representatives when they 'turn a blind eye' to financial transactions that are clearly designed to evade the paying of tax.
An example of such legislation is the UK Criminal Finance Act 2017 which includes the corporate offence of failing to prevent the facilitation of tax evasion.
The offence makes firms liable for the acts of employees and agents where these are deemed to have encouraged, enabled or otherwise assisted a third party in evading the payment of a tax liability. The offence applies to both UK and foreign entities and covers the evasion of both UK and foreign tax liabilities. Note that the Act, like FATCA in the US, asserts a long-arm jurisdiction, which means that the offence does not have to take place within the UK for an offence to have been committed under UK law. Firms

facing investigation for this corporate offence *do* have a defence available to them, provided they are able to show that they had reasonable prevention procedures in place.
Where the UK has led, other jurisdictions may soon follow with equivalent legislation of their own. Firms will need to ensure that they have adequate preventive measures including:

- effective training for all relevant staff
- effective senior management oversight and related procedures for reporting to senior management
- robust, effective whistleblowing policies and procedures including protection for whistle-blowers reporting suspicions of tax evasion facilitation.

PROLIFERATION FINANCING

Increasing international concerns regarding the apparent intentions of certain states (notably Iran) to develop a nuclear weapons capacity led historically to the development of some international accords and country-specific economic sanctions legislation designed to combat the financing of the proliferation of weapons of mass destruction (WMD).
The international measures to combat proliferation financing have much in common with anti-money laundering and counter-terrorist financing. Hence the Financial Action Task Force (FATF), established initially to combat money laundering and subsequently terrorist financing, announced in October 2007 that it was extending its remit to combat proliferation financing, and has since issued guidance on this (see the section on FATF, below). The UN responded with Resolutions in December 2006, March 2007, March 2008 and June 2010, aimed at restricting trade with Iran that might enable or facilitate the proliferation of WMDs.
Up until January 2016, the US, and to a lesser extent the EU, enacted an increasing range of economic sanctions against Iran aimed primarily at its oil and energy, petrochemical and financial sectors. Various EU Council Regulations restricted certain trade with Iran and specifically targeted

proliferation financing by placing increasingly heavy restrictions against dealing with Iran's credit and financial institutions.

The US also took even more restrictive steps, with the passing into law in July 2010 of the Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA). This Act required sanctions for companies that actively invested or intended to invest in Iran's energy sector and was a game-changer as far as sanctions compliance was concerned. No longer was it simply a question of financial institutions having to check whether or not a person, entity or country was 'on a list'. On pain of exclusion from the US financial system, they had to know enough about their clients – and in some cases their clients' clients – and their businesses, to be able to determine whether or not they were engaging in sanctioned activities – something that was not always easy to do. For example, activities that could trigger sanctions included:

- making an investment that directly and significantly contributes to the enhancement of Iran's ability to develop its petroleum resources, of:
  - $20 million or more, or
  - $5 million per investment, totalling $20 million or more in a 12-month period
- selling, leasing, or providing goods or services that could directly and significantly facilitate the maintenance or expansion of Iran's domestic production of refined petroleum products, with:
  - a fair market value of $1 million or more, or
  - an aggregate fair market value of $5 million or more in a 12-month period
- selling or providing Iran with refined petroleum products, with:
  - a fair market value of $1 million or more; or
  - an aggregate fair market value of $5 million or more in a 12-month period
- providing goods or services that could directly and significantly contribute to the enhancement of Iran's ability to import refined petroleum products, including:
  - insurance or reinsurance services
  - financing or brokering services, or

– ships and shipping services, with a fair market value of $1 million or more, or an aggregate fair market value of $5 million or more in a 12-month period.

Such US 'secondary sanctions', which generated legal penalties against non-US persons and entities not subject to that country's 'primary sanctions' under the Iran Transactions Regulations 1996, as supplemented, were brought to an end with the coming into force of the JCPOA (Joint Comprehensive Plan of Action) agreement between the 'P5+1' powers (the US, Russia, China, France, the UK and Germany) and Iran in January 2016. Under JCPOA, Iran agreed not to seek to become a nuclear weapons state (something they had in any event always denied) in return for the lifting of the EU sanctions and the US secondary sanctions and there was a brief period when it seemed that full trade with Iran might resume. However, with the decision by the US government in May 2018 to rescind its participation in JCPOA and the subsequent 'snap-back' of its primary and secondary sanctions, at time of writing the *de facto* position for financial institutions that wish to carry on clearing US dollar payments is that doing business with Iran and Iranian persons and entities remains extremely risky. This is notwithstanding attempts by other P5+1 members to construct alternative channels for facilitating transactions with Iran and the situation remains subject to rapid change in accordance with global and regional geo-political developments.

A DEVELOPING FRAMEWORK FOR THE REGULATION OF CRYPTOCURRENCIES

Chapter 1 looked at the advent of cryptocurrencies and their use in money laundering schemes. At the time of writing, there is no really clear consensus about how to regulate cryptocurrency. There is, for example, no international consensus regarding the legal status of cryptocurrencies.

At one end of the scale are jurisdictions such as Gibraltar, which has been at the vanguard of developments in cryptocurrency regulation and allows for the operation of cryptocurrency exchanges within a well-defined regulatory

framework. Gibraltar does not recognise cryptocurrencies as legal tender but *does* recognise them as tradable commodities and has legislated accordingly. Gibraltar's Digital Technology Ledger Framework was introduced on 1 January 2018 and includes a strong focus on provisions for the detection and prevention of money laundering and terrorist financing. Cryptocurrency exchanges are regulated under the Framework and must:

- register with the Gibraltar Financial Services Commission (GFSC)
- demonstrate that they are operating in line with the principles of the Digital Technology Ledger Framework.

Malta, like Gibraltar, does not recognise cryptocurrency as legal tender but allows for trading in cryptocurrency exchanges regulated under the Virtual Financial Assets Act (VFA). This Act lays down a new regulatory framework for the trade in cryptocurrencies, including specific AML and CFT provisions.

Switzerland is another country that has embraced cryptocurrency, albeit via a different approach from that adopted by Gibraltar and Malta. Rather than develop a new regulatory framework Switzerland has chosen to bring the regulation of cryptocurrencies under its existing AML and KYC provisions. In 2017 the Financial Market Supervisory Authority (FINMA) in Switzerland issued its first licence to a cryptocurrency exchange to operate as a 'directly subordinated financial intermediary'. The issue of the licence brings the exchange under FINMA supervision and recognises its compliance with the provisions of the existing regulatory framework. Countries such as Japan and Australia have also taken steps to strengthen existing AML regulations and to incorporate into them the regulation of cryptocurrencies and the EU Fifth Money Laundering Directive referred to earlier does likewise.

At the other end of the scale are countries like China, which has adopted a very hard-line approach to cryptocurrencies, regulating against them by banning ICOs (initial coin offerings), ordering a freeze on bank accounts associated with cryptocurrency exchanges and introducing a nationwide ban on any cryptocurrency trading. Russia had previously prohibited the use of crypto-currencies but in 2018 executed a volte face towards legalising their use.

At time of writing, other countries, such as Switzerland, Japan and - Australia, have taken the view that existing regulations already cover

unlawful activities such as fraud or money laundering and that these same provisions can extend to activities involving cryptocurrencies. In 2016 the European Parliament presented proposals to set up a task force to monitor virtual currencies and to consider new measures to protect against their use in money laundering and terrorist financing. Many other jurisdictions have, however, indicated that they have no specific plans to regulate cryptocurrencies. Lack of international consensus means that, for the moment at least, in many parts of the world bitcoin and other cryptocurrency operations remain unregulated and outside of central bank control. However, the direction of travel seems to be very much towards the adoption of virtual currency and the technology behind it (if not of the current, main high-profile virtual currencies themselves) as mainstream financial instruments. Accordingly, it would be surprising (absent some major financial scandal) if regulation along the lines of Gibraltar or Switzerland did not follow.

THE FINANCIAL ACTION TASK FORCE (FATF)

The FATF (also known as GAFI – Groupe d'Action Financière, see www.fatf-gafi.org) is an inter-governmental body whose membership as of June 2019 comprised 37 member countries and two regional organisations, as well as a number of observer organisations such as the World Bank and the EBRD. It was set up by the then G-7 Summit held in Paris in 1989 in response to the growing threat posed by international money laundering and was given the task of examining money laundering techniques and trends, setting out measures to combat them and then reviewing the action taken at both the national and international level. As terrorist financing has risen up the international agenda, the FATF's role has naturally extended to encompass CFT as well and its remit was also extended to include the proliferation of weapons of mass destruction (WMDs). It works in close cooperation with various other international bodies, including the IMF, the World Bank and the United Nations.

The FATF effectively has a manifold role at the heart of the overall AML and CFT regime, described below.

- To monitor the progress of countries in introducing AML and CFT measures, using self-assessments and more detailed mutual evaluations. Non-compliant governments have found themselves under heavy moral, political and economic pressure to toe the line through the reviews. For example, in the past, Austria eventually agreed to prohibit anonymous savings accounts as a result of pressure from the FATF, and various countries of Eastern Europe and the former Soviet Union embarked upon urgent national legislative programmes in a very short space of time as a result of their actual or threatened inclusion on a 'Non-Cooperative Countries and Territories' List.
- To review trends, techniques and innovations in money laundering (which has led to annual and specialised money laundering typology reports), and to keep member states abreast of the findings.
- To build a global AML and CFT network by extending the reach of FATF principles. This has resulted in new member countries joining the group; it has also led to the formation of regional FATF-style groups.
- To define and promulgate international standards on the combating of Money Laundering and Terrorist Financing and WMD Proliferation. At the heart of FATF's activities are their recommendations on measures for the combating of Money Laundering and the Financing of Terrorism and Proliferation. Now known as 'The FATF Recommendations' they were last fully revised and refreshed in February 2012.

The FATF Recommendations are available from the FATF website at www.fatf-gafi.org. However, for convenience they are summarised here.

The 40 Recommendations (February 2012)

The 40 Recommendations were first published in 1990, revised in 1996, and were comprehensively updated in 2003 and 2012. The FATF - Recommendations 2012 still constitute the baseline source for details of the Recommendations, with amendments made since 2012 published separately.

The 40 Recommendations were designed to provide a comprehensive plan of action for countries that needed to fight money laundering, terrorist financing and weapons proliferation, encompassing the following key areas:

- AML/CFT Policies and Coordination
- Money Laundering and Confiscation
- Terrorist Financing and Financing of Proliferation
- Preventive Measures
- Transparency and Beneficial Ownership of Legal Persons and Arrangements
- Powers and Responsibilities of Competent Authorities and Other Institutional Measures, and
- International Cooperation.

Countries have diverse legal and financial systems and therefore all cannot take identical measures. The FATF 40 therefore lay out broad principles for countries to implement according to their particular circumstances and constitutional frameworks. They are not a binding international convention, but many countries around the world have made a political commitment to fight money laundering by adopting and implementing the FATF 40 and those who do not face censure and reprisals if they refuse to do so.
What follows is only a brief summary of the recommendations and some of the interpretative notes to provide an overview of the headline requirements. It should not be taken as a substitute for detailed reference to the source document. Notes have been added to indicate the date and nature of amendments made since the 2012 document was published.

A: AML/CFT policies and coordination

Recommendation 1 requires countries to adopt a risk-based approach to combating money laundering and terrorist financing to ensure that resources are as efficiently applied as possible. R1 also requires financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs) to 'identify, assess and take effective action to mitigate their money laundering and terrorist financing risks'.

Recommendation 2 requires national coordination between policy-makers, the FIU, law enforcement authorities, supervisors and others, to ensure that the implementation of policies and activities to combat money laundering,

terrorist financing and WMD proliferation is effectively coordinated domestically.
February 2018: R2 was revised to require the compatibility of AML/CFT requirements and data protection and privacy rules, and to promote domestic inter-agency information sharing among competent authorities.

B: Money laundering and Confiscation

Recommendation 3 requires countries to criminalise money laundering as a specific offence and to apply the crime to 'the widest range of predicate offences'. A predicate offence, in this regard, is a serious offence which, legally, can give rise to money laundering where criminal proceeds have resulted from it. Most notably, the 2012 recommendations require that countries include tax evasion as a predicate offence, which was never the case previously.

Recommendation 4 requires countries to empower their competent authorities (such as police and prosecutors) to identify, trace, freeze, seize and confiscate criminal assets. It also permits countries to confiscate such assets ahead of any criminal conviction which is likely to be sought.

C: Terrorist Financing and Financing of Proliferation

Recommendation 5 requires countries to criminalise both the financing of terrorist acts and the financing of individual terrorists and terrorist organisations, as well as designating terrorist financing offences as predicate offences for money laundering purposes.
October 2015: The interpretative note to R5 was revised so as to clarify that countries must criminalise financing the travel of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning, or preparation of, or participation in, terrorist acts or the providing or receiving of terrorist training.
October 2016: A further revision of the interpretative note to R5 replaced '*funds*' with '*funds or other assets*'; and revised the glossary definition of '*funds or other assets*' by adding references to oil and other natural resources, and to other assets which may potentially be used to obtain funds.

Recommendation 6 requires countries to implement 'targeted financial sanctions régimes' to prevent and suppress terrorism and terrorist financing pursuant to the various UN Security Council Resolutions, for the purpose of freezing terrorist funds and denying their availability to designated persons and entities.

Recommendation 7 requires that countries also implement targeted financial sanctions régimes aimed at preventing, suppressing and disrupting WMD proliferation pursuant, again, to UN Security Council Resolutions.
June 2017: The interpretative note to R7 and glossary definitions of *'Designated person or entity'*, *'Designation'* and *'Without delay'* were revised to bring the text in line with the requirements of recent United Nations Security Council Resolutions and to clarify the implementation of targeted financial sanctions relating to proliferation financing.

Recommendation 8 requires countries to pass laws which prevent the exploitation of NPOs for terrorist financing purposes.
June 2016: R8 and the interpretative note to R8 were revised to clarify the subset of non-profit organisations (NPOs) which should be made subject to supervision and monitoring.

D: Preventive Measures

Recommendation 9 requires that bank (and other financial institution) secrecy laws should be subordinate to the implementation of the FATF recommendations (so that, for example, institutions reporting in good faith cannot be the subject of successful legal actions for damages by customers and clients claiming damages for breach of confidentiality).

Recommendation 10 relates to customer due diligence (CDD). Financial institutions must undertake CDD when:

- establishing business relations
- carrying out occasional transactions above USD 15,000 or certain wire transfers
- there is a suspicion of money laundering or terrorist financing, or
- there are doubts about the truth or adequacy of previously-obtained identification information.

Under Recommendation 10 institutions must:

- identify and verify the customer's identity using 'reliable, independent source documents, data or information'
- identify the beneficial owner of the account (i.e. the natural person or persons who own or control it, or for whose benefit it exists, and behind whom there are no further interests), and understand the ownership and control structure of corporations and other entities to this effect
- understand the purpose and intended nature of the business relationship; and
- conduct ongoing due diligence and transaction scrutiny throughout the course of the relationship to ensure consistency between account activity and stated purpose.

The CDD measures should be determined according to a risk-based approach (examples of which are dealt with in more detail in Chapter 4 of this book) and although customer identification and verification is not required to precede the opening of business relations, this is subject to the risks being effectively managed. An inability to conduct CDD for any reason should effectively prohibit a financial institution from providing the requested services and generate a need to consider the making of a suspicious transaction report.
Recommendation 10 is the subject of an extensive interpretative note containing expanded requirements on CDD for legal persons and arrangements. In particular, it contains a step-by-step process for the establishment of the identity of beneficial owners. Under this process, institutions should first identify the natural person or persons exercising control of the corporation or trust through ownership; failing that, they should attempt to establish those exercising control by means other than ownership (presumably, for example, through secret agreements, commercial arrangements, etc.); failing that, they should establish a relevant natural person who holds a senior management position.

Recommendation 11 requires financial institutions to maintain transaction and CDD records for a minimum period of five years from the date of the transaction (in relation to transaction records) or following the termination

of the business relationship (in relation to CDD records). These records must also be made available to competent authorities within the jurisdiction.

Additional Measures for Specific Customers and Activities

Recommendation 12 deals with politically exposed persons (PEPs) and their family members or close associates and requires institutions to take additional steps to the CDD measures outlined in R10; in particular to put in place systems to determine whether the proposed relationship involves a PEP, to obtain senior management approval for such relationships, to take 'reasonable measures' to establish the source of wealth and the source of funds and to conduct 'enhanced ongoing monitoring' of the relationship.

Recommendation 13 contains a series of requirements in relation to cross-border correspondent banking, under which, in addition to the CDD measures described in R10, financial institutions must obtain information on and understand their respondents' business, reputation, quality of supervision and quality of AML/CFT controls (particularly where CDD on customers have access to 'payable through accounts'), as well as obtaining senior management approval for the establishment of new correspondent relationships and understanding the respective responsibilities of the respondent and correspondent.
Recommendation 13 also prohibits the provision of correspondent services to shell banks.

Recommendation 14 requires countries to establish licensing and registration systems for customers who provide money value transfer services (MVTS) with appropriate penalties for unlicensed operators.

Recommendation 15 requires countries and financial institutions to risk assess new products and delivery mechanisms and technologies for money laundering and terrorist financing purposes and to take steps to mitigate those risks.
October 2018: Insertion of new definitions for 'virtual asset' and 'virtual asset service provider' in order to clarify how AML/CFT requirements apply in the context of virtual assets including cryptocurrencies.

Recommendation 16 relates to wire transfers and is the subject of extensive guidance in the interpretative notes. The headline requirement is that countries must require financial institutions to include both originator and beneficiary information in wire transfers, and that that information should remain with the transfer throughout the payment chain.
There are also requirements for financial institutions to be able to detect wire transfers which lack the necessary information and also to freeze the processing of wire transfers apparently involving designated persons and entities.

Recommendation 17 allows countries to permit financial institutions to rely on third parties to perform CDD steps (other than ongoing due diligence) in certain circumstances. However, the relying institution must retain ultimate responsibility (in legal terms) for the adequacy or otherwise of the CDD measures.

Recommendation 18 requires that countries should compel their financial institutions to implement AML and CFT programmes which, in the case of institutions with overseas branches and subsidiaries, should be to a consistent standard throughout, based on the home country's requirements.
November 2017: Revision of the interpretative note to R18 clarifying the requirements for information sharing in relation to unusual or suspicious transactions within financial groups, including a requirement to provide such information to branches and subsidiaries as necessary for AML/CFT risk management.

Recommendation 19 requires that financial institutions should apply enhanced CDD measures to relationships involving countries which have been designated by FATF as higher risk.

Recommendation 20 requires that financial institutions be under an obligation to report suspicions of money laundering or terrorist financing promptly to the country's Financial Intelligence Unit (FIU).

Recommendation 21 requires that national laws should protect financial institutions and their staff who have reported suspicions of money laundering or terrorist financing in good faith, from civil or criminal liability for breach of confidentiality. Recommendation 21 also mandates

that countries prohibit by law the practice of 'tipping-off' (informing a customer that a report has been filed with the FIU).
November 2017: Revision of R21 to clarify the interaction with the tipping-off provisions required under R18.

Recommendations 22 and 23 contain a range of requirements in relation to designated non-financial businesses and professions (DNFBPs). Basically the CDD and record-keeping requirements set out earlier apply to DNFBPs in designated situations, as do the recommendations relating to internal controls, foreign branches and subsidiaries, higher-risk countries, the reporting of suspicious transactions and tipping-off.
Specifically, the interpretative notes to Recommendation 23 make it clear that lawyers (and accountants providing legal advice) are not required to file suspicious transaction reports in circumstances where the information forming the basis of their suspicion was acquired in a situation which was subject to professional secrecy or legal professional privilege. Furthermore, lawyers are not deemed to have 'tipped-off' a client if they seek to dissuade them from engaging in certain types of activity that might constitute money laundering.

Recommendations 24 and 25 require countries to ensure that information on beneficial ownership and control in relation to legal persons (e.g. corporations) and legal arrangements (e.g. trusts) is available and can be accessed by competent authorities, and that they should also consider measures to make information on beneficial ownership and control available to financial institutions and DNFBPs.
These greatly expanded requirements in relation to beneficial ownership are the subject of an extensive interpretative note which makes it clear that, at the heart of the matter, companies are going to have to be able to draw a distinction between legal ownership on the one hand, and beneficial - ownership on the other, and to appoint 'one or more natural persons resident in the country' to provide information on beneficial ownership to the authorities.

Recommendations 26, 27 and 28 require countries to maintain adequate regulatory and supervisory frameworks for financial institutions and DNFBPs, and set out the minimum standards applicable.

Recommendation 29 requires countries to establish a FIU for the analysis of suspicious transaction reports and the obtaining of further relevant information in relation to money laundering and terrorist financing.

Recommendation 30 outlines the required responsibilities of law enforcement and investigating authorities and emphasises the importance of 'proactive parallel financial investigation' and inter-agency cooperation.

Recommendation 31 details the required powers of law enforcement and investigating authorities, such as their ability to access all necessary documents for use in investigations and their powers to use investigative techniques such as undercover operations, communications interception and controlled delivery (i.e. participating in the handling and delivery of illegal goods and substances for the purpose of obtaining evidence for prosecution).

Recommendation 32 deals with cash couriers, and the requirement that countries should put in place mechanisms to control the cross-border - transportation of cash and negotiable instruments through declaration and/or disclosure systems.

Recommendations 33 and 34 impose obligations on countries to maintain statistics pertaining to the effectiveness and efficiency of their AML/CFT systems and to provide feedback to financial institutions and DNFBPs which will assist them in complying with their obligations, in particular their reporting of suspicious transactions.

Recommendation 35 requires countries to maintain a range of 'effective, proportionate and dissuasive' sanctions against persons and entities which fail to comply with their AML/CFT obligations. These sanctions should also be applicable to directors and senior management of financial institutions and DNFBPs.

Recommendations 36 to 40 then finally cover a range of requirements in relation to international cooperation, including becoming parties to relevant international conventions, mutual legal assistance, cross-border asset freezing and confiscation, extradition and generally providing 'the widest

range of international cooperation in relation to money laundering, associated predicate offences and terrorist financing'.
February 2013, insertion with reference to R37 and R40: secrecy or confidentiality laws for designated non-financial businesses or professions (DNFBP) must not affect the provision of mutual legal assistance except where the information sought is held in circumstances where legal professional privilege or legal professional secrecy applies.

FATF REGIONAL STYLE BODIES AND ASSOCIATE MEMBERS

Several regional organisations and other bodies have been established to carry forward the principles and practices set out by FATF on a more localised/regional basis. They enjoy observer or associate membership status at the FATF and are:

- The Asia/Pacific Group on Money Laundering (APG)
- The Caribbean Financial Action Task Force (CFATF)
- The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- The Grupo de Accion Financiera Sud America (GAFISUD)
- The Eurasian Group (EAG)
- The Middle East and North Africa Financial Action Task Force (MENAFATF)
- The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL)
- The Inter-Governmental Action Group against Money Laundering in West Africa (GIABA).

All the groups analyse the latest money laundering and terrorist financing trends which have been detected in their region and all look to the FATF as the global leadership organisation in these fields.

OTHER RELEVANT INTERNATIONAL BODIES

International Monetary Fund (IMF)

The IMF has long been involved in international efforts to combat money laundering at a national level, and after the events of 9/11 it intensified and extended the remit of these activities to include combating the financing of terrorism. As a collaborative institution with a near-universal membership of countries (it has 187 members), the IMF is perhaps a natural forum for countries to share information and develop common approaches and appropriate policies to deal with such issues.

The IMF has also brought to bear its capabilities in the assessment of member states' financial sectors, and the provision of technical assistance to help countries strengthen their financial sectors. The Financial Sector Assessment Programme (FSAP), established in 1999, is a joint effort with the World Bank and is designed to provide member countries with a comprehensive evaluation of their financial systems as a whole, rather than those of individual financial institutions. The FSAP aims to alert the national authorities to weaknesses in their systems, and to help them design countermeasures to reduce those weaknesses. The IMF and World Bank are also involved in policy development in the counter-terrorist financing arena and author publications on various issues of concern and interest, including reference guides, handbooks and working papers on topics such as the operation of Financial Intelligence Units, legislative drafting and the impact of terrorism on financial markets.

The IMF has taken a number of specific steps to assist countries in strengthening their anti-money laundering counter-terrorist financing provisions. In March 2004, the IMF Executive Board agreed to make AML and CFT assessments and technical assistance a regular part of IMF work, and to expand this work to cover the full scope of the FATF recommendations. In 2009, the IMF launched a donor-supported trust fund to finance technical assistance in AML/CFT.

Basel Committee on Banking Supervision (BCBS)

The Basel Committee was established at the end of 1974, and comprises central bank (or banking supervision authority) representatives from 27

countries including the US, the UK, Japan and a number of EU states. The Committee formulates broad supervisory standards and guidelines and recommends statements of best practice in the expectation that individual authorities will take steps to implement them through detailed arrangements – statutory or otherwise – suited to their own national systems. Its main guidance documents cover areas such as transparency in payments messages, account opening and customer identification, customer due diligence and international cooperation.

The Egmont Group

The Egmont Group was set up in 1995 to facilitate international cooperation and in its ongoing work aims to support the growing number of Financial Intelligence Units (FIUs) set up by various countries in recent years. Its purpose is broadly to provide a forum through which FIUs can improve their national AML programmes. Any FIU which considers itself to comply with the criteria of the Egmont Group, of being a central, national agency responsible for receiving (and where permitted, requesting) disclosures of financial information, and analysing and disseminating such information to the competent authorities as appropriate, is eligible to apply to become an Egmont member FIU.

The Wolfsberg Group

The Wolfsberg Group is an association of 13 global banks, which aims to develop financial services industry standards for know-your-customer, AML and CFT policies. The group first came together in 2000 (at the Château Wolfsberg in north-eastern Switzerland – hence the name) to draft anti-money laundering guidelines for private banking in the wake of some very negative money laundering scandals which had affected the industry. *The Wolfsberg Anti-Money Laundering Principles for Private Banking* was subsequently published in October 2000 (and revised in May 2002). Since then the group has published various papers on a wide range of areas including Terrorist Financing Correspondent Banking, Monitoring, Screening and Searching and the Risk Based Approach. The group also publishes FAQs on a range of specific issues including beneficial ownership, Politically Exposed Persons (PEPs) and intermediaries and

various iterations of its 'Correspondent Banking Due Diligence Questionnaire' (CBDDQ) for use in onboarding respondent banks and other financial institutions as customers. (www.wolfsberg-priciples.com)

IAIS and IOSCO

Beyond the banking sector, international bodies such as the International Association of Insurance Supervisors (IAIS) for the insurance industry, and the International Organization of Securities Commissions (IOSCO) have issued guidance to members on best practice in the combating of money laundering and terrorist financing.

KEY REQUIREMENTS FOR FINANCIAL INSTITUTIONS

There is by now a fairly well-defined suite of activities which, taken together, denote current international best practice in anti-money laundering and counter-terrorist financing, and these revolve around the core areas below. More detailed information on best practice approaches is provided in Chapter 3.

Name screening

Before entering into a business relationship, prospective customers' names must be checked against published lists of persons and organisations suspected of being connected with terrorism. Financial services must not be provided to those on the lists.

Risk assessment

Before entering into a business relationship, prospective customers must be assessed as to the degree of money laundering and terrorist financing risk which they pose, and must thereafter be the subject of appropriate risk-based procedures and controls. Risk factors to be considered include:

- location of customer and/or transaction
- type of customer (individual, corporate, trust, etc.)
- nature of customer's business
- age/period of existence of customer
- countries where customer typically conducts its business
- counterparties of customer
- product profile and sales distribution channels.

A detailed explanation of a risk-based approach to money laundering and terrorist financing is provided in Chapter 4.

CDD and EDD

Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) must be undertaken where necessary, on a risk-sensitive basis, including:

- *Identification*. Evidence and verification of the customer's identity must be obtained prior to the provision of services.
- *Business purpose*. Details of the business purpose of the relationship must be obtained.
- *Beneficial ownership*. Where this is unclear, beneficial ownership must be ascertained, the test being one of significant interest and control.
- *Ongoing monitoring* of accounts on a risk-sensitive basis and scrutiny of transactions to ascertain whether they are consistent with the stated purpose of the account.
- *Prohibition on opening accounts for shell banks*. Banks without a physical presence in the jurisdiction where they are incorporated, and which are otherwise not part of a larger group constituted in a well-regulated country, are designated as 'shell banks' and may not be banked. It follows from this that where it is unclear whether or not a bank is a shell bank, financial institutions must make reasonable efforts to establish whether or not it is, and thereafter to act accordingly.
- *Simplified due diligence* may be allowed under certain circumstances, for example where customers are counterparties from well-regulated jurisdictions, or where a customer has been introduced by such an entity.

More information on CDD and EDD implementation is provided in Chapter 4.

Suspicion reporting

On a risk-sensitive basis, 'suspicious' transactions must be reported to the authorities and cooperation extended to the authorities in the investigation of such reports. Specifically, financial institutions must not make customers or third parties aware that such reports have been filed.
More information on different typologies, the features that characterise them and how to recognise these in financial business is provided in Chapter 6.

Record-keeping

Customer and transaction records must be retained and kept available for inspection for five years from the date of the end of the relationship (in the case of customer records) and five years from the date of the transaction (in the case of transaction records).

Staff training

Training must take place on a regular basis, in which relevant staff are trained in:

- how to recognise a potentially suspicious transaction
- what to do if they become suspicious
- their own legal obligations and those of the financial institution where they are employed
- the procedures and controls in place for dealing with AML/CFT issues within the financial institution.

More information about staff training and examples of tried and tested training and awareness techniques is provided in Chapters 3, 6 and 8.

Cooperation with relevant authorities

Cooperation must be extended, within the parameters defined by law, to law enforcement agencies in the investigation of suspected money laundering and terrorist financing. In suspected terrorism cases, in particular, it is especially important that financial institutions are able to produce records quickly in response to requests.

Responsiveness to international findings

Financial institutions must take account of information made available from reliable sources which is relevant to their assessment of money laundering and terrorist financing risk. For example, if a country appears on the International Cooperation Review Group list of countries issued periodically by the FATF, which are either non-compliant with the FATF 40 or which have strategic deficiencies in their compliance regimes, then financial institutions should reassess and amend their risk control procedures accordingly in respect of business involving that country.

KEY COMPONENTS OF A NATIONAL AML/CFT FRAMEWORK

As part of the mutual evaluation regime, on an ongoing basis FATF conducts detailed assessments of the extent to which the AML/CFT regimes of different countries do or do not meet the international standards which it has set out in the FATF 40.
The basic requirements, however, for the institutional framework in each country are as follows, and each country must have the following.

Core legislation

The country must have primary statutes which criminalise the process of money laundering and terrorist financing, permit the seizure and confiscation of criminal and terrorist assets, impose criminal penalties (fines and imprisonment) for breaches of the law and which, in all other respects, comply with the requirements laid out in the FATF 40 and the

various international conventions and regional treaties to which the country is a party.

Regulations or statutory instruments and interpretative notes or guidance

The country must have regulations or statutory instruments which address in detail the legal requirements contained in the core legislation, and which set out the various steps which regulated parties (i.e. financial institutions and the other 'gatekeepers' who are charged with AML and CFT duties) must take in order to fulfil their obligations. The regulations must cover such issues as:

- risk assessment
- customer identification and due diligence
- account and relationship monitoring
- suspicion reporting
- records maintenance
- internal controls
- staff training.

Along with other key areas identified in the FATF 40, it is not enough that regulations simply be issued; they should also be the subject of interpretative guidance which assists regulated firms in understanding and applying them.

Regulatory bodies

The country must have a regulator or regulators that have powers to inspect firms' compliance with laws and regulations and to compel improvement. Regulators must have powers to censure and impose fines and other punishments in order to give 'teeth' to their inspections. It follows from this that the staff of these regulatory bodies must be knowledgeable about the AML and CFT matters which are the subject matters of their inspections.

Financial Intelligence Units

Countries must have centralised units to receive and analyse reports of suspicions of money laundering and terrorist financing under the legislation and regulation, to build knowledge and expertise of money laundering trends and methods within their country, and to make this intelligence available to the state enforcement bodies (see below) for the purpose of taking effective action.

Law enforcement agencies

Countries need to empower police forces or other investigative agencies to investigate money laundering and its underlying crimes, and terrorist financing and the plots being funded by it. Again, officers within these agencies need to be sufficiently skilled and knowledgeable in this regard, in order to be able to fulfil their tasks successfully. The area is typically so complex that designated agencies may be required to conduct specialised tasks such as asset tracing, asset seizure or terrorist surveillance.
Ultimately, the purpose of law enforcement is to catch criminals, seize their assets and bring cases to court, so they need to work closely with the next component of the national AML/CFT regime, below.

Prosecutory authorities

Countries need to have prosecutory authorities that can work with the police to prepare and bring to court cases of money laundering and terrorist financing. Again, specialist knowledge and expertise are required for the lawyers and case specialists involved in reviewing and preparing the cases for court, and presenting/advocating them in court.

Judicial and penal system

Countries must have judges, courts and prisons capable of administering justice according to the law. This means the system must have the capacity and resources to try cases and appeals which are brought before the courts and to do so within a reasonable time, and to have effective state institutions for punishment, once convictions have been obtained.

Integrity

Finally, and perhaps most importantly, it is worth mentioning here that the ‘golden thread’ running through all of the above is the requirement that a country’s AML/CFT regime and apparatus should have integrity at both the institutional and the individual level, and that decision-making should be free from bribery and corruption. Equally, the state should provide the necessary resources to protect, as far as humanly possible, individuals from threats, coercion and violence at the hands of the criminal community whose power they are trying to attack.

3

The Role, Structure and Positioning of the AML/CFT Compliance Function

Structure and culture

AML/CFT best practice

Best practice in higher-risk products and services

IT systems

The use of artificial intelligence

Training, communication and awareness

A ‘pro-business’ approach

STRUCTURE AND CULTURE

Core activities for the AML/CFT role

These can be summarised as follows:

- securing senior management support (a Board member should be responsible/held accountable for AML/CFT)
- the completion of an Enterprise Risk Assessment (ERA)
- producing, monitoring and updating policies and procedures
- providing an advisory support capability to the front line
- receiving, analysing and investigating internal disclosures of suspicious activity from staff
- making external disclosures of suspicious activity to the authorities
- using international findings and UN and other watchlists
- staff training and awareness
- regular reporting on AML and CFT to senior management (e.g. MI, testing results, annual report)
- responding to information requests from competent authorities
- general assurance and oversight of the bank's overall AML/CFT effort.

Key policies and procedures

These should include the following as a minimum:

- name screening (client acceptance) to include 'list management'
- risk assessment methodology (client acceptance)
- identification (client acceptance)
- due diligence and enhanced due diligence
- transaction surveillance

- sanctions and prohibited transactions
- suspicion recognition and reporting
- records maintenance
- training, awareness and communication
- incorporation of international findings
- staff and third-party screening.

Position of the AML/CFT role within the organisation's structure

The exact place of the AML/CFT compliance role within the overall structure of the organisation is not prescribed internationally, and so will depend upon any national requirements and on the preferences of the organisation and its senior management.

It is now recognised that to ensure an effective AML/CFT regime it is essential that a very senior manager of the organisation is given responsibility and accountability for the AML/CFT or the wider Financial Crime Compliance function. This should preferably be a member of the Board of the organisation.

In the largest international banks, the position of Head of AML and CFT is a senior position which is well remunerated and offers enough direct access to senior management to be able to function effectively. Typically, the AML/CFT function will fit within one of two models:

1. *As part of a wider financial crime function*. In this model, AML and CFT sit within a specialist unit which also deals with fraud prevention and other types of financial crime such as insider trading, market manipulation, tax evasion, Anti Bribery and Corruption and proliferation financing. This model is likely to become more prevalent as Open Source Intelligence (OSINT) and data analytics relating to financial crime assume a heightened importance in generating functional capability and efficiency.
2. *As part of a wider legal and compliance function*. In this model the AML/CFT function sits within a wider unit which, apart from AML and CFT, also deals with issues such as:

    - compliance with other banking rules and laws

- compliance with the organisation's code of conduct dealing with issues such as conflicts of interest and other ethical matters relating to integrity and anti-corruption.

It is of course also possible for the unit to sit completely independently, as a statement of the importance attached to it. If that is the case, then the reporting line of the head of the unit should be at least to the senior manager responsible and accountable for AML/CFT, which should be at least at Executive Director level and possibly to the Chief Executive Officer, in order to avoid the risk of the unit being bypassed in important decision-making processes.

AML/CFT units are rarely part of the audit function. This is because they must themselves be subject to scrutiny and oversight in relation to the effectiveness of the way in which they perform their duties. This would not be possible if they were part of the audit function, whose job it is to provide management with assurance that different functions in the organisation are doing their jobs efficiently, including the AML/CFT function.

The so-called 'three lines of defence model' for AML and CFT sees the organisation setting up three tiers of protection against the various risks posed. These are:

- *First line of defence – at line management level.* Relationship managers, branch and corporate and private banking managers and supervisors and their frontline staff comprise the outer armour of the organisation's defences. They are relied upon to be aware of the risks and to apply policies and procedures as they have been laid down, for example in relation to issues such as identification and onboarding, transaction surveillance, name screening and suspicion reporting.
- *Second line of defence – AML/CFT unit.* The AML/CFT unit itself forms the second line of defence. The unit exercises general oversight of all AML and CFT activities within the organisation including:
  - handling internal suspicion reports
  - designing policies and procedures
  - providing and conducting training and awareness
  - engendering senior management support
  - monitoring and reviewing the application of policies within the business units through assurance visits and relevant management

information (MI).

The unit should use audit-type skills to conduct assurance activities such as interviewing, testing and sampling to satisfy itself that policies are being applied successfully. Nevertheless, such activities will not constitute formal audits in governance terms. This can only be provided by the audit department.

- *Third line of defence – audit department.* The organisation's audit department provides the third line of defence, conducting full, independent audits not only of business units (which should also include AML and CFT checks and sampling) but also of the AML/CFT function itself, to provide assurance to the Board and Audit and Risk Committees that it is doing its job properly. Indeed, stand-alone AML/CFT audits should be considered in a risk-based approach.

Organisation of the AML/CFT role

In terms of who does what within the AMT/CFT function, in a small organisation one or two people may handle everything from business queries to training, to writing policy, to arranging IT support for name screening, etc. As an organisation becomes larger and more complex, however, this clearly becomes inappropriate and a division of responsibilities becomes necessary.

The precise nature of the division, if not prescribed by local law, is a matter for the Head of the AML/CFT function to decide. For example, a Head in a reasonably large organisation might split the responsibilities of the function as follows or, where resources are tight, allocate clusters of them to individuals:

- regulatory and FIU liaison and reporting
- receipt and review of internal Suspicious Transaction Reports (STRs) and data analytics from alert engines associated systems
- sanctions, blacklists, name screening and client acceptance
- policy, training and international compliance
- day-to-day operational advice to business units
- second line assurance activities
- Management Information (MI) compilation.

The very largest organisations will need to operate matrix structures in which different roles are performed across multiple products in different business streams across multiple jurisdictions (if the organisation is expanding internationally). These structures may, for example, see different heads of AML/CFT distributed through the organisation on a business or geographic basis, with double reporting lines to both the general managers of those businesses and into a main, centralised AML/CFT function sited in head office.

In such cases, the more complex the structure needs to become, the more important it is that there is great clarity as to who is responsible for what – in particular the statutory responsibilities laid down under national law and, of course, clarity within the organisation as to whom suspicious transactions should be reported.

Importance of a strong compliance culture

Although all core activities in the AML/CFT role are important, there is one activity in particular which is paramount: securing senior management support. Compliance starts from the top and without the commitment of senior management the role of the AML/CFT Compliance Officer becomes that much more difficult, and some might even say impossible.

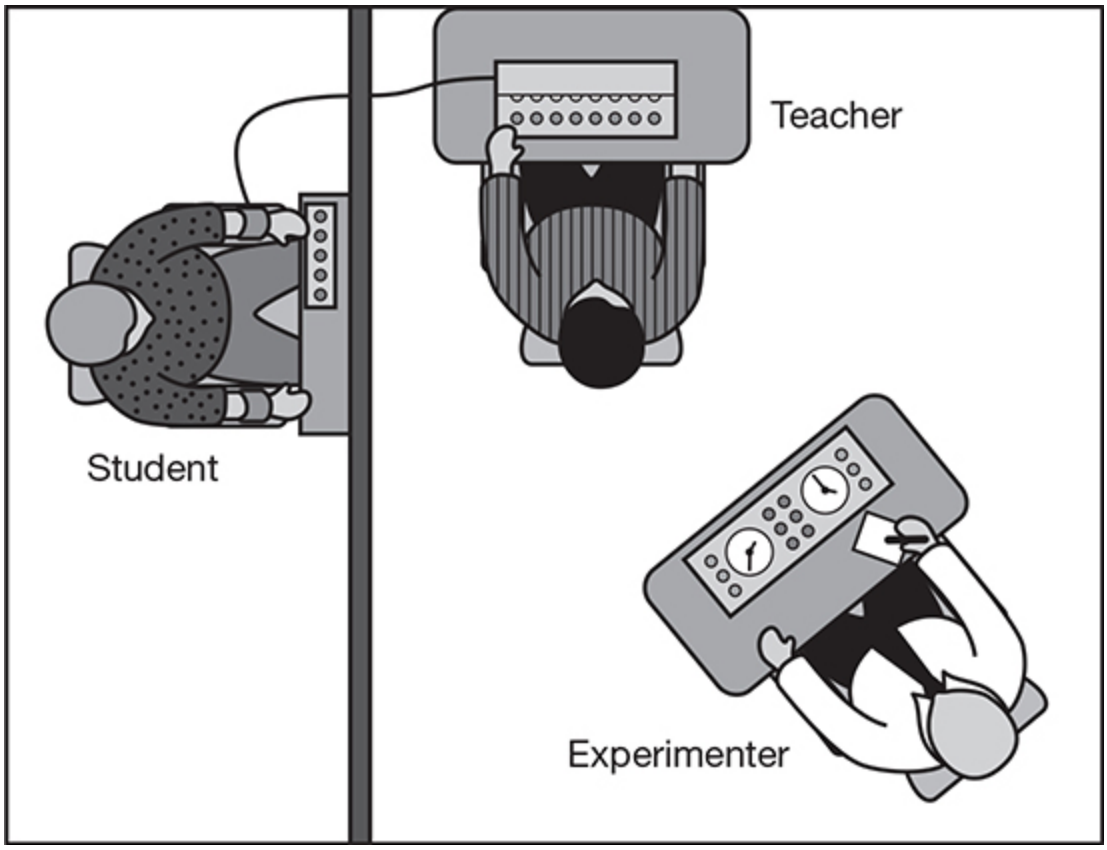
Why is this? The answer is that the senior managers in organisations occupy positions of such power that effectively they determine the culture of the organisations which they lead. Whether it is because subordinates want to impress them, or because they are fearful for their jobs, or because they act purely from habit, the reason may differ from case to case. But the general indication is that people's propensity to follow orders at work and 'go with the flow' is extremely high.

What is the evidence for this? Much research has been done in this area, but two psychological studies conducted in America in the 1960s are particularly worthy of mention. The first, undertaken by Stanley Milgram, placed subjects in a situation where they thought they were taking part in experiments to determine a person's capability to follow simple instructions, with a small electric shock being administered if the person followed the instruction incorrectly. They were assigned the task of the 'teacher' and had to administer these small electric shocks to the 'student' who was situated on the other side of a pane of glass, the two being

separated by a contraption described as an ‘electric shock machine’. The arrangement is shown in Figure 3.1.

In fact there were no electric shocks and the real subjects of the experiment were the ‘teachers’ who were being asked to administer what they believed to be increasingly severe electric shocks to the ‘students’ (who were in fact actors) for no other reason than that they had got the answer to a simple question wrong. As the ‘shocks’ increased, the ‘students’ displayed increasing amounts of distress. Milgram’s ‘teachers’ were accompanied by authority figures in white coats (the experiments were conducted at Yale University in the US) to whom they frequently appealed during the experiments for permission to stop. Always, however, the answer came back calmly but firmly to proceed with the administration of the ‘electric shocks’. Milgrim was interested to test how far people would go in following instructions from an authority figure. The results were extraordinary. Significant percentages of the subjects would proceed to administer what they believed to be lethal electric shocks to the ‘students’. This led Milgram to his chilling conclusion: ‘A substantial proportion of people do what they are told to do, irrespective of the content of the act and without limitations of conscience, so long as they perceive that the command comes from a legitimate authority’. (*Source*: www.stanleymilgram.com/quotes.php)

Figure 3.1 **Milgram’s famous experiment**



If Milgram's experiment dealt with people's propensity to follow orders, then the experiments conducted by another American psychologist named Solomon Asch graduated more towards people's willingness (or otherwise) to speak out in a group when they believe that something is wrong. Asch sat his single subjects in groups with 11 others, all of whom knew the true purpose of the experiment, with only the subject unknowing. A group would be shown different images of lines of differing lengths and were asked to state which line was longer, which was shorter, etc. Each member of the group would state his or her opinion in turn. The subject was always in the latter half of those asked, such that the majority in the group had already given their opinion by the time it came to the subject. The differences in the line lengths were quite obvious. For a couple of rounds in each group, the majority of those asked 'Which was the longer line?' gave the correct answer, as did the subject. However, at a certain point the majority gave wrong answers and, again, in surprisingly high numbers the subjects would agree with the majority even though the evidence of their own eyes was telling them quite clearly that the opposite was true.

These two experiments demonstrate what most of us have probably already experienced: that in organisations people tend to do as they are told and are, by and large, very reluctant to speak out when they receive an instruction which they believe to be 'wrong'. Applying this to an AML/CFT culture it becomes easy to see how such a culture would be weak and ineffective unless senior management is not only '*talking* the talk' but also '*walking* the talk', i.e. insisting upon adherence to necessary standards, even where that may mean giving up a short-term revenue gain.

Example

The case of the rising star

In one financial institution there was a policy which stated very clearly that: 'In case of doubt we do not hesitate to reject potential customers or terminate business for AML concerns, even if it means losing profitable business. Consequently, we accept from staff a critical attitude with regards to new customers.' A young relationship manager, aware of the policy, was publicly criticised by his manager in team meetings when he raised concerns about certain new customers and the origin of their wealth. He was told, 'Go and join the Compliance Department, you'd fit in better there than you do here,' and he was overlooked for promotion and received a smaller bonus than some of his colleagues. He raised the matter privately with the Compliance Department who, after getting nowhere with the business manager concerned, escalated the matter to the CEO, explaining that in its view it was essential that the business manager should get a clear message from the CEO that the AML policy was meant to be followed in practice. The business unit run by the manager was, however, performing extremely well. Its revenues were at record levels and undoubtedly the manager was partly responsible for this.

In spite of several subsequent requests, the CEO took no action, choosing rather to issue a generally worded memo to all staff about the importance of the AML policy. A month or two later, another manager in the business unit informed Compliance that the manager had treated the matter humorously in a subsequent team meeting, quipping that the CEO needed him more than he needed the Compliance Department. The second manager said, 'Everyone knew what had happened and everyone knew what the outcome had been. From that moment on nobody was in any doubt that, whatever the AML policy said, the view of their manager, backed by senior management at the highest level, was that whenever the policy jeopardised profits, it could be overlooked.'

In another case, however, another senior manager became aware from the available Management Information (MI) that CDD error rates in one business unit were way above the tolerance accepted by the organisation on one area. The senior manager decided that no new business was to be taken on by that unit until the errors had been rectified and all staff were re-trained on client acceptance requirements. Now that's what we mean by 'walking the talk.' This model of a 'compliance culture' is depicted in Figure 3.2, which describes the typical ways in which management deals with staff who either observe or break organisational rules (vertical axis) and hit or miss their targets (horizontal axis). The key test of organisational culture comes in the lower left quadrant. What does management do with people who meet their targets but break the rules?

Figure 3.2

Observes rules	Coach	Reward
Ignores rules	Fire	?
	Misses targets	**Exceeds targets**

Gaining senior management support

Genuine support from senior management is so essential that nothing good or effective will be achieved without it. There are some obvious things that you can do on a personal level to foster support from senior managers, such as:

- communicating with senior managers regularly, both orally and in writing
- regularly sharing information with senior managers about different aspects of AML/CFT compliance (but don't become a bore)
- inviting senior managers to contribute to discussions about AML/CFT compliance (e.g. at department meetings or training sessions)
- ensuring that news of positive developments reaches key senior people, while also ensuring that any 'bad surprises' are flagged up as early as possible, together with options and recommendations for resolution

- developing good relationships with regulators whose views senior management must take note of.

However, AML/CFT Compliance Officers must appreciate that it is insufficient simply to write lots of memos and other communications pointing out what the laws and regulations say. To achieve *real* commitment and all the good things that flow from it the AML/CFT function must adopt an approach that is business-focused; a partnership one that casts AML/CFT compliance as something that is there to help the business *succeed*, rather than as a 'blockage' to be got around or ignored.

The foundation stone for your business-focused approach should be a desire to *achieve* (or, if a great one exists already, to *maintain*) the right culture within the organisation. This will not be a culture in which the business views compliance as being the Compliance Department's problem, but rather a culture in which the business takes *ownership* of compliance for itself and incorporates it seamlessly into its business processes, with the support and help of the CEO and senior management team and the Compliance Department. This type of culture is typically achieved by:

- a business-owned governance structure that puts a heavy emphasis on business responsibility for compliance
- a complete set of policies that can be 'seamlessly' integrated into each business unit's operating procedures and that apply in practice as well as on paper
- adherence to current best practice, demonstrating a commitment to anticipate and keep pace with a rapidly developing regulatory environment
- IT (including Artificial Intelligence (AI)) systems designed to assist the organisation in fulfilling its obligations and in meeting its AML/CFT objectives
- a continuous training and communication programme emphasising the importance of AML/CFT compliance and equipping staff so they can comply with both organisational policy and national law
- a proactive, business-friendly approach from AML/CFT Compliance Officers, with an emphasis on efficient and effective suspicion reporting management.

Business ownership

What practical steps can you, the Compliance Officer, take to embed responsibility for AML/CFT compliance within the business itself? In terms of corporate governance there are a variety of possible measures, outlined below.

Policies

Corporate policies should state clearly that responsibility for compliance lies with business units. For example:

> **'Business heads are responsible for ensuring that procedures and controls commensurate with these standards and guidelines are in place for all units under their control.'**

Anti-Money Laundering Group (AMG)

It is not sufficient that business managers' responsibility for compliance should simply be incorporated within policy documentation. Managers will need reminding on a constant basis that responsibility is theirs. A good mechanism for achieving this is a regular AMG meeting, comprising the heads of the major business units concerned, briefed to discuss AML and CFT issues specifically. The AMG should be chaired by the chief executive or general manager and would consist of the heads of businesses, the Chief Operating Officer, the Compliance Officer and any other key personnel. An example agenda is shown below:

Example

AMG AGENDA

for the meeting to be held on [*date*] *at* [*place*]

1. Minutes and action points from last meeting on [date].
2. Update on Suspicious Activity Reporting (Compliance Officer) and 'live issues' from business units.

3. Progress on staff training and awareness and other initiatives within the anti-money laundering strategy (each Business Head).
4. Other Assurance and Management Information results (e.g. SAR - numbers, training stats, transaction monitoring/name screening stats).
5. Policies and procedures – any points arising.
6. Legal and regulatory update – including global/international developments (Compliance Officer/MRO).
7. A.O.B.
8. Next meeting.

Chaired by the Chief Executive Officer, or in his absence the Deputy CEO or Chief Operating Officer (COO).
For attendance – Heads of Businesses, COO and any other key personnel agreed.

Link to performance

Responsibility for AML/CFT compliance should also be built into the organisation's performance management framework, thus ensuring that observance of AML/CFT good practice is one of the measures against which managers' work performance is assessed. Specific AML/CFT objectives can be included within a business manager's overall personal performance objectives. Similar provisions can be cascaded down into the objectives of more junior staff. This will highlight the importance of AML/CFT compliance and signals clearly that bonuses will be at risk if compliance performance objectives are ignored. An example for a senior business manager might be as follows:

Example

Anti-Money Laundering objectives

During the assessment period, actively to assist the bank's drive against money laundering and to provide business leadership on money laundering prevention by:

- taking effective measures to ensure that the business complies with the letter and spirit of AML policies and procedures at all times
- attending and contributing at the senior management AML meetings
- implementing action points agreed upon and decisions made at AML meetings
- attending and, where appropriate, introducing staff training sessions on AML
- achieving a score of 18 or more in the 20 questions AML self-assessment test administered by compliance.

Compliance Champions

It is rare that an AML/CFT function will have sufficient resources and personnel to have an employee present in each business unit. Even if it did, as representatives of the Compliance function such employees may be viewed as separate from the business. A 'Compliance Champion' therefore is an employee who sits within the business and undertakes certain specific activities such as:

- distributing information (e.g. articles or briefing notes) about a particular topic received from the AML/CFT Compliance Officer
- helping in the organisation and delivery of formal training sessions and training programmes on AML- and CFT-related topics, in conjunction with the Compliance Department
- providing the AML/CFT Compliance Officer with direct feedback on the effect of certain policies and procedures on the business, and making suggestions for improvement
- periodically meeting up with the AML/CFT Compliance Officer and Compliance Champions from other business areas to discuss

compliance issues and problems and recommend practical solutions which will work at the point of business

- delivering short, informal briefings on compliance-related topics at, for example, business team or management meetings.

Because of their proximity to the business, Compliance Champions are unable to undertake any kind of independent assessment of compliance standards. This must be done either by the Compliance Officer or the Audit Department in accordance with the three-line defence model discussed earlier.

Communication of requirements

Setting up a business ownership structure as outlined above requires communication – from the Compliance Officer to the Chief Executive, and from the Chief Executive to business heads. Shown below are examples of the documents that might have a role to play in such a strategy, based around the three themes of:

1. creating a 'culture of compliance'
2. embedding responsibility for compliance within business units
3. the development and maintenance of sound AML and CFT policies and procedures.

Clearly the Compliance Officer should discuss their overall approach with the CEO beforehand and obtain their support for the approach, but otherwise these memos are practical documents which, when taken in conjunction with a senior management presentation and a staff briefing, for example, could form the basis of an effective communication strategy to explain the business ownership approach advocated here.

Example

MEMO TO CHIEF EXECUTIVE OFFICER RECOMMENDING ACTION STEPS ON MONEY LAUNDERING RISK

To: [ ], Chief Executive Officer

From: [ ], [Compliance Officer] [Risk Officer] [Title]
Date: [ ]
Re: Money laundering risk – Action going forward

1. I refer to our discussions regarding the above, and now set out formally, as requested, my observations on how [Name] Bank should best deal with the management of money laundering and terrorist financing risk going forward.
2. In common with other regulated banks and financial institutions in [Country], we have been complying with [Central Bank] regulations regarding the opening of customer accounts, the mandatory reporting of certain transactions and the reporting of unusual or suspicious transactions for some time. However, in view of international trends in relation to money laundering prevention, which clearly indicate:

    - a significant tightening of regulatory standards
    - a significant increase in the reputational damage likely to be suffered by defaulting banks, and
    - a significant increase in likely penalties to be imposed upon defaulting banks – including possible denial of access to the financial system in key areas such as the US, EU, etc.

    I believe we (the senior management team) now need to adopt a **strategic approach** to this issue, and to formalise the general increase in awareness which we have all felt, into a concrete and comprehensive plan of action which is visible to staff, customers and regulators alike. The medium- and long-term aims and benefits of doing this will be substantial and will include:

    - a reduced risk of use of our bank by criminal elements

- in the event that such use does occur against our best efforts, a much greater ability to defend ourselves from criticism, due to our having initiated voluntarily a programme of best practice measures which complement the minimum regulatory requirements
- as a result, a strengthening of our overall risk management capability.

3. I believe that our strategy should concentrate on three broad and complementary areas or 'themes' of action, and I outline what these are below, together with some of the practical measures which we can implement to bring them to life.

THEME 1: BUILDING 'A CULTURE OF AWARENESS' AMONG STAFF IN RELATION TO MONEY LAUNDERING

In best practice benchmark organisations, all staff – but particularly those in key areas – are aware of the risks posed by money laundering and terrorist financing, and of the steps which are expected of them in trying to prevent and/or to identify it. This means much more than just making the relevant laws and policies (see below) available to staff. It means imbuing them with an instinctive vigilance which they, while remaining hungry for business, then apply to all customers and all transactions. Actions to achieve this objective would include:

- regular training (suited to job, grade, etc.)
- regular distribution of relevant materials and resources
- periodic surveys to measure awareness
- periodic assessments to test knowledge
- suitable treatment of the issue during the staff induction process
- 'stress testing' of vigilance in, for example, branches

- overt and unequivocal senior management support for the anti-money laundering message.

THEME 2: EMBEDDING RESPONSIBILITY FOR ANTI-MONEY LAUNDERING COMPLIANCE WITHIN BUSINESSES

In organisations where the primary responsibility for ensuring anti-money laundering compliance is seen to rest with the Compliance/Risk function, businesses never fully accept their role in preventing money laundering. Management time is wasted as businesses and risk functions adopt 'us and them' postures. Risk is increased as, freed from responsibility for the ultimate outcome, businesses attempt to accept business which they may be less than sure about. Genuine revenue opportunities are lost as compliance/Risk functions, feeling pressured and under attack, veto business which might otherwise be accepted.

In best practice benchmark organisations, however, primary responsibility for compliance lies with the businesses, where such compliance is seen as an integral part of the business cycle. Actions to achieve this objective would include:

- specific CEO memorandum to business heads, setting out their responsibilities [see 'BusinessACMem.doc']
- policies and procedures which specifically include statements of business responsibility and accountability [see 'Policy'.docs (various)]
- ensuring that policies and procedures are observed day-to-day, by rewarding compliance and punishing non-compliance
- the launch of a senior management group, called the Anti-Money Laundering Group (AMG) to oversee [Name] Bank's overall anti-money laundering effort [see 'BusinessACMem.doc]; such group to include heads of businesses

- inclusion of a specific anti-money laundering objective in the personal job objectives of business heads and all other staff, with performance against this objective being included in a person's annual appraisal, and such objective to include a requirement to take effective steps for ensuring that businesses comply with the letter and spirit of our AML policy and procedures
- during anti-money laundering training, a continuous emphasis on the personal responsibility of staff for the prevention and identification of money laundering
- the appointment of specific people at a more junior level within businesses to act as 'Compliance Champions' (this role to be 'double hatted' with their existing roles), assisting the Compliance Officer/Risk Manager with various tasks such as training and the dissemination of relevant materials and resources.

THEME 3: THE [DEVELOPMENT OF] [MAINTENANCE AND ENHANCEMENT OF OUR] ANTI-MONEY LAUNDERING POLICIES AND PROCEDURES

We must [develop] [maintain and enhance our] policies and procedures in key areas connected with the fight against money laundering, so as to ensure that [Name] Bank's position on anti-money laundering is clearly spelled out, and that staff have clear standards to follow. These must be adapted to be specifically relevant to each type of business and should [be updated to] cover the following issues:

- screening against international, regional and national 'blacklists' and the management of those lists
- customer risk assessment, identification and verification

- additional ‘know your customer/business’ procedures, according to risk
- transaction surveillance, according to risk
- records retention
- identification of suspicious transactions
- reporting of suspicions
- handling of customers under suspicion
- use of ‘material deficiency’ findings
- internal auditing and compliance monitoring
- pre-employment (third-party) screening
- staff education and training.

4. Our policies and procedures must be living documents, which are updated regularly so as to remain relevant to new products and risk areas, and which are an integral part of the way in which each business is run.

5. The three themes complement each other. A strong culture of awareness among staff will make it easier for businesses to assume responsibility for compliance, just as the assumption of that responsibility will help develop the desired culture. Clear, relevant and up-to-date policies and procedures will help – and be helped by – both.

6. If you are in agreement with the above, the next step would be for us to have discussions with the business heads concerning this new strategy, before convening the first meeting of the AMG to agree a more detailed plan of how and in what order to launch and implement the various initiatives.

Sincerely, etc.

Example

CEO's MEMO RE: BUSINESS RESPONSIBILITY FOR ANTI-MONEY LAUNDERING COMPLIANCE

To: All Business Heads [and e.g. COO]

From: [ ], Chief Executive Officer

Cc: [ ], Compliance Officer

Date: [ ]

Re: 1. Business responsibility for anti-money laundering compliance
2. Launch of Anti-Money Laundering Group (AMG)

The purpose of this note is to outline the responsibilities which you and your businesses bear in relation to the prevention and detection of money laundering and terrorist financing in [Name] Bank in [Country] , and to set out the terms of reference for a new senior management group which I have decided to form, to be called the Anti-Money Laundering Group (AMG), to assist in the planning and implementation of a comprehensive anti-money laundering strategy for [Name] Bank in [Country].

1. **Business responsibility for anti-money laundering compliance**
   Primary responsibility for compliance lies with the business, and not with the Compliance Officer/Risk Manager. As discussed with each of you individually, I view your responsibilities as follows:

   - To cooperate with the Compliance Department in the devising and implementation of anti-money laundering and counter-terrorist financing policies and procedures suitable for your business, and to keep them updated and relevant to new products and changes to local laws and circumstances and international conditions.

- To ensure that these policies, procedures and laws are observed day-to-day, for example by rewarding compliance with them, and by punishing non-compliance.
- To ensure that a specific anti-money laundering objective (in the form attached at the Appendix) is included within your own personal job objectives, and that suitably adapted versions appear within the objectives of other key identified staff, with performance against this objective being included in annual appraisals and such objectives to include a requirement to take effective steps for ensuring that the business complies with both the letter and spirit of our AML policy and procedures.
- To ensure that anti-money laundering and counter-terrorist financing training is undertaken for all relevant staff, with a repeated emphasis being placed on the personal responsibility of staff members for the prevention and identification of money laundering.
- To appoint, in consultation with the Compliance Officer/Risk Manager, a specific person within your business, to act as a 'Compliance Champion' (while this role may be 'double hatted' with their existing role it is essential you ensure they have the necessary time and resource to act as a Champion), assisting the Compliance Officer/Risk Manager with various tasks such as training and the dissemination of relevant materials, information and resources in relation both to money laundering and to compliance generally.
- To ensure that relevant staff, when considering customers, business and transactions, give due consideration and weight to money laundering and terrorist financing risk. In particular, that

they do not abdicate their own personal responsibility for ensuring the suitability of business for onboarding.

2. **Launch of Anti-Money Laundering Group (AMG)**

The AMG will be the senior body within [Name] Bank in [Country] for the management of money laundering and terrorist financing risk. Consisting of the heads of businesses, [the chief operating officer (COO)], the Compliance Officer/Risk Manager and myself, it will have the following terms of reference:

- The broad objective of the AMG will be to implement an anti-money laundering strategy, specifically:
  - to help create a 'culture of awareness' among staff within [Name] Bank in [Country], in relation to money laundering risk;
  - to help embed responsibility for anti-money laundering compliance deep within the businesses of [Name] Bank in [Country]
  - to help [develop] [maintain and enhance] effective anti-money laundering policies and procedures in [Name] Bank in [Country]
  - to help ensure that [Name] Bank in [Country] takes considered and appropriate action in response to [Name] Bank, national or international issues arising in connection with money laundering.
- The AMG will meet at least once every two months, or more frequently should it be required.
- The standard agenda for AMG discussions will be as per the document entitled AMGAgenda.doc, but other topics may be

included as required.

The first meeting of the AMG will take place on [date] at [time], when we will attempt to establish priorities and timings for the various initiatives.

In conclusion, I cannot over-emphasise the devastating effect which even inadvertent involvement in a money laundering and/or terrorist financing scandal would be likely to have on our business and reputation [in the current environment]. Nor can I overstate the critical importance of your providing firm leadership on this issue within your respective businesses [and functions]. I know I can count on you to work with me to ensure that our anti-money laundering strategy is a success.

Sincerely, etc.

APPENDIX – FOR INCLUSION IN STAFF PERFORMANCE OBJECTIVES

During the assessment period, actively to assist the Bank's drive against money laundering and terrorist financing, and to provide business leadership on money laundering and terrorist financing prevention by:

- attending and contributing at the senior management AMG meetings
- implementing action points agreed upon and decisions made at AMG meetings
- punishing instances of non-compliance appropriately and ensuring that non-compliance is not rewarded
- attending at and, where appropriate, introducing, staff training sessions on money laundering
- achieving a score of 80 per cent or more in the money laundering self-assessment test administered by compliance/risk management.

AML/CFT policies, procedures and systems

With the assistance of the AML/CFT Compliance Officer, businesses will need to implement complete policy, procedure and system solutions to the AML/CFT risks which they face. The precise scope and content of these policies, procedures and systems will be influenced by local law and regulation, but in order to comply with international standards they will need to deal with at least the following areas:

- *Customer acceptance and name screening.* How the organisation takes on (or 'onboards') a new client and determines that the client is not on any international alert lists. This will also include list management (e.g. what lists to apply) as well as any 'internal' lists (e.g. customers who have been rejected/exited to stop them re-entering the organisation).
- *Client Due Diligence (CDD) and risk assessment.* How the organisation checks that clients are who they say they are and how they determine the level of money laundering and terrorist financing risk posed by each client (see Chapter 4 for more details).
- *Know Your Customer (KYC).* How the organisation builds its knowledge of each customer's transaction and business pattern so as to be able to discern any unusual activity.
- *Monitoring and transaction surveillance.* How the organisation monitors its clients' accounts and the overall relationship for unusual and potentially suspicious activity.
- *Suspicious transaction reporting.* How the organisation detects and reports (internally and externally) transactions or relationships which are potentially suspicious (including its policies to deal with customers who are under suspicion).
- *Mandatory reporting.* If the law requires this, how the organisation reports transactions of a certain type or above a certain threshold to the authorities.
- *Record-keeping.* How the organisation creates and stores customer records in accordance with national and international legal and regulatory requirements.
- *Ongoing screening.* How the organisation screens its existing client base on a regular basis to ensure that it is free of individuals and entities named on relevant lists of proscribed persons.

- *Training and awareness.* How the organisation raises awareness of AML/CFT risks and provides staff with the knowledge and skills necessary to combat them.
- *Material deficiency findings.* How the organisation detects, responds to and implements the findings of relevant international bodies (e.g. FATF, UN) in relation to areas or geographies of AML/CFT risk.
- *Staff and third-party screening.* How the organisation screens key staff ahead of their employment for AML/CFT risk as well as third parties, e.g. those connected to trade transactions or contractors to the organisation.
- *Audit and assurance.* How the organisation assures itself that the AML/CFT compliance function and policies and procedures are operating effectively through second line assurance activity as well as regular management information (MI).

AML/CFT BEST PRACTICE

The World Bank and the IMF have produced guides to best practice, grounded in the FATF recommendations and in the Basel Committee on Banking Supervision's international standards. In addition, there is relevant guidance from other industry-specific bodies and relevant sources including IAIS (insurance), IOSCO (Securities), the Wolfsberg Group (international and private banking), the Joint Money Laundering Steering Group (UK consultative body) and the US Department of Treasury Anti-Terrorist Financing Guidelines (re. charities), summarised in composite form below.

Customer identification and due diligence

The global CDD and KYC standard outlined here derives from the World Bank and IMF guidance and from the FATF recommendations together with associated regulatory guidance issued in countries such as the UK and US. The standard can be used as a benchmark for the banking sector, as well as a best practice reference point for other financial sectors.

How far should the KYC policy extend?

Whatever regime is introduced at the headquarters of an institution must be applied to its branches and to any majority-owned subsidiaries, both - domestically and internationally, unless it clashes with local law in that jurisdiction. If there are differences in regulatory standards between home and host countries, then the more comprehensive/stronger of the two should be applied.

Who is a customer?

Banks need to establish at the outset whether the person with whom they are dealing is acting on their own behalf, or whether there is a beneficial owner of the account who may not be identified in their paperwork. If a bank is aware or suspects that the customer is representing a third party, it must carry out due diligence on that third party as well.

Third parties may be organisations or legal entities as well as individuals. It can be particularly difficult to establish who the beneficial owner is when 'tiered ownership' is involved, with a whole pyramid of companies controlling one another and in some cases a parent company at the top. Again, appropriate due diligence is necessary in such a situation to find out the precise identity of the parent entity.

Customer acceptance procedures

It is necessary for banks to be able to identify which potential new customers represent a high risk in terms of money laundering and the financing of terrorism, by developing high-risk profiles against which they can be measured. Standard risk indicators for money laundering will include factors such as:

- the customer's country of origin (e.g. from a country notified by the International Cooperation Review Group (ICRG) of the FATF, or a country habitually associated with the production, transit or processing of illegal narcotics)
- the type and country of business activity (e.g. arms, casinos, diamonds, jewellery, money or crypto exchange)
- any linked accounts, and whether or not they have a high-profile position and/or are 'politically exposed'

- the kinds of products which the customer wishes to use, and whether they are of particular use to someone wishing to launder money (e.g. no notice restrictions on withdrawals).

As regards terrorist financing, it simply is not possible to produce a meaningful profile for an individual terrorist financier, but clearly issues surrounding the general profile of an account will be relevant, such as:

- known connections with a conflict area or country associated with terrorism
- business interests in or with such countries/areas
- frequent money transfers to and from such areas and travel to and from them (such as with associated charities and non-profit organisations)
- complex ownership structures leading back to individuals or businesses with connections to such places.

Senior management approval

The risk-based approach generally means that the bank can afford to exercise reduced due diligence with low-risk customers. The IMF/World Bank guidance recommends that the rigidity of the acceptance standards should be in proportion to the risk profile of a potential customer. However, when new customer business deemed to be 'high risk' is up for consideration, the onus should be on the *senior* management to make the decision as to whether or not such business is appropriate for the bank to take on.

Customer identification

Bank staff should verify any new customer's identification to their satisfaction before an account is opened. Customers are not allowed to open accounts in fictitious names, and nor are numbered accounts permitted unless the usual customer ID procedures and supporting documentation are used as a matter of course.

Once they come to request identification documents, banks should ask for those that are hardest to forge. For individuals the most suitable are - official documents such as passports, driving licences, personal ID cards or tax identification documents. An institution's procedures should specify

which of these or other documents might be acceptable for different individuals. For legal entities the suitable documents specified might include a certificate of incorporation, the business's registered address, its tax identification number and whatever other proof of the business's legitimacy as an entity is required.

When an intermediary – for example a trustee, financial adviser or nominee – is opening an account or carrying out a transaction on behalf of an individual or a corporate customer, then unless legally sanctioned 'passporting' procedures apply (e.g. as in the EU, where business introduced by other EU-regulated entities may be assumed to have been correctly identified already), the financial institution needs to take steps to verify the identification of the beneficiary. This will include the following information:

- the name and legal form of its organisation
- its registered or legal address
- the names of the directors and the principal beneficiaries
- the details of the agent acting on behalf of the organisation and the organisation's account number with the agent
- the regulatory body to which the organisation answers.

There are sometimes legitimate reasons why a customer may not be able to provide preferred identification such as a passport or driving licence.

Since the purpose of customer identification is not to exclude legitimate customers from having access to financial services, an institution's identification procedures should therefore include some alternative means of identifying customers to a satisfactory standard.

Detecting forgery

Particular care needs to be taken with the risk of forged identities, since this is a mechanism known to be used increasingly by terrorists, as well as criminal groups. For example:

- When dealing with a new customer face to face, it is important to check that the photo supplied is of the person actually opening the account, and that the date of birth given is realistic in the light of their appearance (an obvious point, but one easily missed in a frenetic retail environment).

- If bank statements from two financial institutions are presented as supporting evidence, check that the two show different transactions (one known method is to 'cut and paste' transactions to manufacture a second statement).
- Does the ethnicity of the name seem to match that of the customer?
- Is the content of each document consistent throughout (e.g. do the dates match)?
- Are the document margins straight? (Crooked margins are a red flag for forgery)
- Are there any other signs that the document has been tampered with?

Originator and beneficiary information on funds transfers

Funds transfers of any description should be accompanied by accurate and meaningful originator and beneficiary information – including name, address and account number – and that information should remain with the payment all the way along the payment chain.

Maintenance of CDD and KYC information

Knowing your customer is an ongoing exercise, which means that banks have to put effort into keeping records up to date – for example, if there are material changes in the way an account is run, or in the event of significant transactions being made on the account. Organisations should consider having set timescales for such updates as well as significant trigger events (e.g. the organisation becomes aware that the customer has changed their countries of business, or that there has been a change in ownership and control).

Low- vs high-risk accounts and transactions

As discussed above, the risk-based approach requires financial institutions to assess the AML and CFT risks attached to different types of customer profile. Similarly, financial institutions need to weigh up the potential for different kinds of product to be misused for criminal activities. For instance, a wire transfer service is a more obvious choice than a 90 days' notice deposit account in this respect (though long notice accounts can have their criminal uses too).

For lower-risk categories of customer (e.g. public companies or government enterprises) financial institutions may be able to scale down or simplify the due diligence requirements, for example by requiring fewer details about the business relationship or expected transactions. Nonetheless *all* customers, even lower-risk ones, should be required to prove and verify who they are. For higher-risk categories, banks should take additional precautions when they carry out customer due diligence. We look more closely at the various types of higher-risk customers, products and services in Chapter 4.

Record-keeping requirements

Minimum periods

As we have already seen, when intelligence services or regulatory authorities are tracing the evidence trail behind a money laundering or terrorist financing discovery, the availability of customers' financial records (current and/or historic) can be a significant help in the detection and prosecution of the individuals involved. Moreover, the very fact that records are kept as a matter of course is believed in some cases to deter would-be criminals from their original illicit plans.

FATF Recommendation 11 sets a minimum international standard for the period over which banks and other financial institutions must retain records of the identification data obtained from customers (at least five years beyond the end of the customer relationship) and records of the customers' transactions (at least five years beyond the date of the transaction). National regulation and institutional policy must therefore enforce this or a higher standard of record-keeping. The regulators of any country may, of course, choose to extend the minimum five-year holding period for institutions based in their jurisdiction.

Type of information retained

The information retained by banks as a matter of course should include:

- a customer's name, address and account number
- the date and nature of each transaction
- the currency and amount involved

- any other information that is routinely recorded by the bank and could be relevant in piecing together a criminal evidence trail.

Reporting obligations

Suspicious Transaction Reports (STRs)

STRs are the mainstay of anti-money laundering programmes. They place the onus on financial institutions to spot suspicious or anomalous activities among the daily flood of transactions, and despite the difficulty in detecting financing activity at the front end of the terrorist financing chain, they have their place in countering terrorist financing, too. As FATF puts it:

> **'If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should . . . report promptly its suspicions to the financial intelligence unit.'**
>
> *Source*: www.fatf-gafi.org copyright © FATF/OECD. All rights reserved.

However, a financial institution should, under no circumstances, alert the customers under scrutiny to the fact that their behaviour has been monitored and reported to the authorities.

Characteristics of suspicious activities

'Suspicious activities' can take numerous forms, but many will share certain broad-brush characteristics. Most obviously, as far as money laundering in particular is concerned, they tend to involve transactions out of step with the usual patterns seen on the account in question. So any complex or unusually large deals, or unusual transactions without any obvious commercial or lawful purpose, should be viewed as potentially suspicious and reported internally and, if appropriate, thereafter to the relevant authorities.

As far as terrorist financing is concerned, a variety of indicators may give cause for concern, ranging from problems with identification documents through to, for example, unusual signing arrangements, evidence of ulterior control by undisclosed parties, and wire transfer activity which shows signs of manipulation or structuring in order to evade reporting requirements or disguise ultimate sources of funds information.

Extent of reporting duties

How far does the reporting organisation have to go in its reporting duties? An STR simply comprises the factual details of a transaction or series of events; there is generally no reason why the reporting bank, insurer or other financial institution should necessarily know anything about *what* it thinks may be wrong, only that it thinks that something *may* be wrong. Given that a United States' Office of the Comptroller of Currency (OCC) guide identified more than 200 predicate crimes for money laundering, of which terrorist funding is just one, anything else would be an unrealistic expectation. In any case, anything more than initial attempts to try to clarify details by asking leading questions of the customer could amount effectively to a tip-off that their account was under scrutiny. Financial institutions' obligations to report are therefore based on nothing more concrete than suspicions, and once they have filed an STR then any further investigation is generally left in the hands of the authorities, although reporting institutions may cooperate with the authorities in order, for example, to further their investigations and, hopefully, bring about successful prosecutions.

Currency transaction reporting

Given the enduring attractions of cash for money laundering or terrorist financing purposes, which in many ways goes against the global trend towards the use of plastic and the electronic movement of money, there is arguably a case for reporting any cash transaction above a certain threshold, on the basis that if everybody does it, such mass data can then be used for the purpose of trend analysis. The FATF 40 Recommendations go no further than suggesting that countries should consider the feasibility and utility of implementing such a regulation. Some jurisdictions have taken this step (including the US, Russia, and the countries of Eastern Europe and the former Soviet Union), but others have not, notably the UK and some other Western European nations.

For example, the US requires that financial institutions record and report to the authorities any currency or bearer instrument transactions of $10,000 or more as a matter of course, and Australia has a similar A$10,000 threshold. The UK regime is entirely suspicion based, and has no automatic reporting threshold, although CDD procedures are required for one-off transactions above the legal threshold.

Reporting obligations for transactions involving cash do apply across the board where same-day multiple transactions – known as 'smurfing' – occur. This process is used by money launderers as a means of avoiding a designated reporting threshold by breaking up the movement of cash into many smaller transactions. If smurfing is suspected, financial institutions need to report the entire series of transactions to the authorities, even though individually they do not breach any reporting threshold that may exist. Additionally, a single transaction could also be suspected on the grounds that the customer was trying to evade the reporting requirements, if it was for slightly less than the relevant reporting threshold. Again, in such cases the bank should look more closely at the transaction and file a report if it is suspicious.

Duty of confidentiality vs duty to report suspicion and/or other transactions

An important consideration as regards the whole principle of filing reports to the authorities on customer transactions is the concept of what are known in the US as 'safe harbour' laws. These are laws that protect financial institutions and their staff from criminal or civil liability arising from the alleged breaking of confidentiality or secrecy laws, provided they report suspicious transactions *in good faith*; that is, without malice.

Controls and independent audit

All organisations covered by a country's AML and CFT laws need to set up their own internal policies and procedures to protect themselves against the risk of being criminally exploited in either way. A critical aspect of these internal controls is an independent audit function (whether based within the firm or brought in from outside), which is separate from the AML/CFT compliance function and therefore able to test objectively the adequacy of the overall compliance arrangements. This is in addition to any second line assurance activity the AML/CFT compliance function may carry out.

Staff training and awareness

Equally significant is the requirement for ongoing staff training. While regular training programmes on how to recognise potential money

laundering activity and what action to take have become a well-established feature of fully compliant financial institutions, much less attention is paid to the specifics of terrorist financing within the formal financial system. In the words of one (anonymous) senior compliance figure in the EU banking industry: 'There's not sufficient focus on terrorist financing generally. Banks should be able to point to specific CFT action that staff should take and training which they have undergone.'

Name screening

Prior to 9/11, the sanctions lists produced by international or national authorities focused mainly on specific countries or regimes, with the aim of prohibiting fund transfers to the sanctioned country and freezing the assets of the government, businesses and residents; or else they targeted known political figures. Since that date, the composition of the lists has changed, as thousands of individuals and organisations suspected of having terrorist links have been added to the lists in response to a plethora of terrorist attacks, criminal investigations, civil wars (e.g. Syria), invasions (e.g. Crimea) and human rights abuses (e.g. Sudan). This is in addition to the additional, business activity-based due diligence required by Iran-targeted measures such as CISADA referred to in Chapter 2.

Accessing and making effective use of the lists is a challenging operational requirement for all financial institutions. There are many sanctions lists available. The UN produces a broad global list, applicable to all member states, while the EU consolidated list comprises names featuring in the annexes to various EC regulations. In addition, individual countries may have their own domestic sanctions regimes.

For the US financial sector, the sanctions authority is the Office of Foreign Assets Control (OFAC). The OFAC list should include names listed under the UN sanctions regime, but it will not necessarily contain EU sanction targets. Use of the OFAC lists as well as the national and UN sanctions lists is necessary for all foreign financial institutions dealing directly with the US, and for this reason is generally undertaken by all large banks and indeed should be undertaken by any bank undertaking dollar business.

Pre-lists

In addition to these formal sanctions lists, from time to time the authorities issue warning lists of names deemed to be a source of concern to those institutions where those people are believed to have accounts, even though there are no legally binding sanctions attached at this stage. The purpose of the warning lists is to enable financial institutions to move immediately to freeze the target assets if or when these names are subsequently added to formal sanctions lists.

Initial and subsequent screening

Financial institutions are required to run all new accounts of any sort against the current updated versions of the relevant lists, and similarly to screen all existing accounts on a regular basis. Wire transfers should also be screened as a matter of course (see below) to establish that no person or entity whose name appears on a list is the recipient of the funds. It is a key operational responsibility for the AML/CFT Compliance function to decide which lists their organisation must watch and how often. This latter point will be a matter for each firm's internal policy, and a reflection of its size and character. For instance, a small insurance firm might choose to scan its database monthly, whereas an international bank opening 10,000 to 20,000 new accounts each day would need to scan on a daily basis. Effectively this means that such institutions must have systems and software that can do this for them and there are a multitude of solutions on the market.

Other than sanctioned persons, the lists are often supplemented with those individuals considered to be politically exposed. This assists organisations in the early identification of such potentially high-risk customers.

Finally, organisations should also consider the necessity to search for the existence of any negative information pertaining to their potential customers. This may not be a direct sanction, but the fact that they may have been involved in other activity that would be of concern (e.g. previous or current alleged criminal activity). As such, many organisations conduct media searches looking for and considering any 'adverse or negative' media that may exist.

This, again, should be risk based and would often be considered only for the higher-risk-rated customers.

Name match vs target match

Lists should contain any alternative name spellings and aliases used by the suspects in question, but of course it is not possible to conclude that just because someone has a name that features on a sanctions list, that they are the wanted individual. There is a distinction between a 'name match', where the organisation has matched the name of an account holder with the name of a target included on a list, and a 'target match', where the organisation is satisfied that the account held is that of the actual target of the financial sanctions; that is, the suspected 'bad guy'.

Action when information is inconclusive

Full details of any target matches should be reported to the authorities and any affected accounts frozen immediately. However, it has to be said that target matches are a relative rarity. It is more likely that a name on the database will match with an entry on a sanctions list but there will be no conclusive evidence that it is the same person or organisation. In that case it is the financial institution's job initially to look more closely at the CDD and KYC information and customer profile on record, and to assess it against the details available on the list. If it is not possible either to confirm or to clear the customer's name on the basis of available information the financial institution may be able to seek guidance from the sanctions authorities, but in the meantime it is faced with the intractable problem of how to treat the customer's account. Given the consequences and penalties of making a mistake, many financial institutions will take the view that they have no choice but to adopt the somewhat brutal policy of blocking an account until they have satisfied themselves that they do indeed only have a name match. They will prefer to deal with the customer's lawsuit rather than a regulatory enforcement action or a criminal prosecution.

It is in these circumstances that the importance of painstakingly and -diligently collected and updated CDD and KYC information becomes all too clear, not to mention software programs that can analyse such data against list information and, for example, produce 'target match' probability scores.

Effective compliance with name screening requirements

As well as conducting the screening process on all new accounts, on existing accounts as often as is necessary and on wire transactions and one-off non-customer transactions, financial institutions need to establish and

maintain an effective programme to ensure compliance with the sanctions authority in question. This should include:

- the existence and observance of written procedures for checking transactions against the relevant lists
- open communication lines between internal departments
- regular staff training
- an annual, in-depth audit of the compliance function.

Other considerations include arrangements for maintaining current sanctions lists and distributing them throughout every subsidiary or branch office, both domestically and overseas.

False positives

As well as situations where the available facts are inconclusive, there are also those situations where financial institutions will actually determine, erroneously, that their customer is the person named on the list – the dreaded 'false positive' scenario.

In such circumstances it is essential that financial institutions should be capable of demonstrating that even if the outcome was wrong, they followed their full and correct procedure and carried out checks with any other parties involved (e.g. with a remitting bank). It is vital to keep clear records of the decision-making process leading up to any action taken.

In summary, it is essential that the organisation has clear procedures for which lists to apply, how often and the action to be taken, including escalation, when a 'hit' occurs.

BEST PRACTICE IN HIGHER-RISK PRODUCTS AND SERVICES

As discussed earlier, one of the fundamental tenets of a risk-based approach is that financial institutions should make judgements about the risks of misuse attached to each relationship and should then focus the greater part

of their attention in those areas where the greater risks lie. In this regard, specific attention should be paid to the following.

International correspondent banking accounts

Correspondent accounts may be maintained between banks, for use in making transactions for customers or between themselves. They are overwhelmingly above board, but certain cross-border correspondent arrangements are at risk of misuse by money launderers and terrorist financiers (the assumption being that due diligence and KYC will be dealt with by the respondent bank in the country of origin). Such accounts maintained with banks based in lightly regulated countries are particularly vulnerable, as they may offer a route for people or organisations to access the global financial system while sidestepping more rigorous checks.
As the IMF/World Bank guidance points out, before entering into such a cross-border arrangement, any financial institution should make an assessment of the respondent bank in question, establishing:

- its location
- the nature of its business
- the purpose of the proposed account
- the bank's reputation
- the quality of its supervision
- the extent of its in-house AML/CFT policy and training provisions.

The importance of the above cannot be over-emphasised in the training provided to relevant staff. If 'payable-through accounts' are to be used, then the financial institution needs to ensure that the respondent bank will verify the identity of its customers and carry out ongoing due diligence on them. More generally, the respective responsibilities of the banks should be established and documented beforehand. Correspondent banking is another area where senior management should take responsibility for approving the business relationship before it actually gets going.
Banks should not set up correspondent banking arrangements with organisations located in certain FATF designated high-risk jurisdictions, nor with so-called 'shell' banks (banks which are unconnected with any effectively regulated financial system and which are incorporated in a

jurisdiction where they have no physical presence or actual staff operations).
In addition to the IMF/World Bank, the Wolfsberg Group has produced standard forms that many banks apply for correspondent banking due diligence. These are the Correspondent Banking Due Diligence Questionnaire (CBDDQ) and the Financial Crime Compliance Questionnaire (FCCQ).

Electronic and digital banking

There has been a rapid and dramatic expansion in non-face-to-face business as a result of the development of financial information services and product delivery via electronic means, including ATMs, telephone and internet banking. Although there is no inherently greater risk involved in applications received by phone or internet than in, say, applications by post, a combination of other factors typically aggravate the risks involved.
For example, it is possible to make an application instantaneously, at any time and from any location; it is also easier to make multiple fictitious or anonymous applications without any additional risk and with less danger of detection. Physical documents are not typically required as part of the application process, therefore making it relatively easier to apply by using a stolen identity. All these factors increase convenience for criminals or terrorist groups, and correspondingly, the risks to financial institutions. However, FATF leaves it to individual jurisdictions to work out and put in place appropriate regulatory measures for their financial institutions.
The updated guidelines on customer identification provided by the UK's Joint Money Laundering Steering Group (JMLSG) are an interesting example of the approach being adopted in some quarters. The JMLSG takes the view that:

> **'The extent of verification in respect of non-face-to-face customers will depend on the nature and characteristics of the product or service requested and the assessed money laundering risk presented by the customer . . .**
>
> **The standard identification requirement (for documentary or electronic approaches) is likely to be sufficient for most situations. If, however, the customer, and/or the product or delivery channel, is**

assessed to present a higher money laundering or terrorist financing risk – whether because of the nature of the customer, or his business, or its location, or because of the product features available – the firm will need to decide whether it should require additional identity information to be provided, and/or whether to verify additional aspects of identity.

Where the result of the standard verification check gives rise to concern or uncertainty over identity, or other risk considerations apply, so the number of matches that will be required to be reasonably satisfied as to the individual's identity will increase.'

Source: www.jmlsg.org.uk

The guidance goes on to provide examples of the additional checks that institutions might use to mitigate, in particular, impersonation risk, but leaves it to the institution to determine how and when these will be applied Additional checks could take the form of, for instance (again, depending on the perceived risk presented by the customer), electronic checks as well as documentary evidence, or a written communication to the customer's verified home address, or requiring a form to be completed and returned by post.

Wire transfers

Electronic transfers pose particular concerns for financial authorities and regulatory bodies. FATF's Recommendation 16 and the Interpretive Note thereto sets out in detail the steps that financial institutions should take when sending money electronically:

- Subject to *de minimis* thresholds (which cannot be higher than US$/€1,000) cross-border and transfers should contain the names of both the originator and beneficiary and their account numbers used for processing the transaction (or a unique transaction reference number, if accounts are not used in processing), plus the originator's address or national identity number or customer identity number, or date and place of birth.
- When a single originator bundles a number of transfers destined for various beneficiaries in another country into a single file, and sends

them all together, there is no need to include full originator information on every transfer, provided that the batch file contains all the relevant originator and beneficiary identification details, as above.

- Domestic transfers must also include all the originator information, as above, unless the originating bank is capable of providing this on demand, in which case all that needs to accompany the money is an account number or some other effective means by which to identify the originator. 'On demand' means within three days of the originating bank receiving the request for information from the receiving bank or the authorities, as the case may be.
- Ordering, intermediary and beneficiary financial institutions all have responsibilities for ensuring that the requirements of R16 are met and for identifying and dealing appropriately with wire transfers which do not contain the necessary information.

Private banking

Private banking relationships are set up not only by wealthy individuals and Politically Exposed Persons (PEPs) but also by law firms, investment companies, investment advisers and trusts. Particularly with regard to money laundering, private banking is viewed as a potentially high-risk sector of the banking universe for various reasons – not least because of the typical levels of wealth, the complexity and sophistication of financial services available (in particular, so called 'secrecy' products), and the number of advisers and intermediaries that may be involved in a client's financial affairs. Often, too, the very purpose of starting a private banking relationship is to hide wealth and put it out of reach (whether from corrupt authorities, probing journalists or a vengeful spouse) – a process which is just as effective for criminal proceeds as it is for legitimate funds.

On the other hand, private bankers are likely to have more proactive and personal relationships with their client than would be the case in retail banking, and may therefore have additional insights into anomalous account activity. In this regard it is important to remember that the wealthy client issuing execution-only instructions for transfers of funds between various investments and offshore vehicles could just as easily be a terrorist sympathiser and financial donor, as a genuine client, or a criminal money launderer. Because private banking relationships can be so complex, it is

also important that there are effective systems in place within each bank to monitor and report suspicious activity, and that this can be done based on a client's total activities.

Standards for private banking have been largely driven in recent years by the Wolfsberg Group of international banks, which has drawn up a set of best practice guidelines for global private banking. These set out as the basic principle for client acceptance the requirements that banks will accept only those clients whose sources of wealth and funds can be reasonably established as being legitimate, and whose beneficial ownership is clear. It is the responsibility of the individual sponsoring private banker to make sure this is the case and, indeed, to be alert to suspicious activities on an ongoing basis. Importantly, say the Wolfsberg principles: 'Mere fulfilment of internal review processes does not relieve the private banker of this basic responsibility.' (www.wolfsberg-principles.com)

In addition, the principles address other key areas, as follows.

Client identification and due diligence

Crucially, client identification requirements under Wolfsberg extend beyond the actual named client to the beneficial owners of account assets. The private banker is expected to understand the structure of companies and trusts sufficiently to establish who are the main players involved, and they must make a judgement as to whether to carry out further due diligence on the individuals and companies concerned. Due diligence must include:

- the client's reasons for opening the account
- the client's expected levels of account activity
- details of the business or other economic activity that has generated the client's wealth and an estimate of net worth ('source of wealth')
- details of the sources of funds to be paid into the account upon opening and on an on-going basis.

References or other corroboration of the details are also required, where this is possible, and it would normally be expected that a client would meet their banker face-to-face before opening the account.

Enhanced due diligence for higher-risk accounts

Extra caution is necessary, as would be expected, in cases where a client's money was sourced in high-risk or lightly regulated countries, or where the client is involved in an area of business known to be susceptible to money laundering activities, or where the client is known to send funds to countries associated with terrorist activity or where the client donates to causes in such countries.

PEPs (who tend to favour the bespoke nature and privacy of private banking arrangements) also require additional due diligence (see below), and senior management must approve any new relationship with a PEP. Suspicious transactions (which may include large cash transactions, any account activity out of line with the customer profile, or 'pass-through' transactions) might be identified in a number of ways beyond the usual monitoring of the account. Suspicions might be triggered, for example, through third-party information from the media about a client (see adverse media comments above), meetings with the client, or personal knowledge about factors such as the political situation in the client's country. The onus, according to Wolfsberg, is on the private banker to keep abreast of the 'bigger picture', as well as gaining and maintaining a thorough knowledge of the customer and their situation.

Specific counter-terrorist financing principles

The Wolfsberg Group supplemented its original principles, which focused on money laundering and other financial crimes in relation to private banks, with a further statement on best practice dealing with countering terrorist financing. This highlights the importance of name screening:

> **'The proper identification of customers by financial institutions can improve the efficacy of searches against lists of known or suspected terrorists [applicable to that jurisdiction].**
>
> **To that end, it expands on existing identification, acceptance and due diligence best practice. Banks need to implement name-screening procedures and report any matches to the authorities; in addition, they need to look at ways of speeding the retrieval of information about a customer if it is required.'**

Source: www.wolfsberg-principles.com

Enhanced KYC policies should be in place for any customers involved in business sectors widely misused by terrorist groups, such as alternative remittance systems. Due diligence should be more extensive and rigorous on new business applications from such customers, and monitoring should be increased on both existing accounts and on those new accounts that meet the acceptance criteria. As a basic principle, banks should limit their business relationships with remittance businesses, exchange houses, bureaux de change and money transfer agents to those which are subject to appropriate AML/CFT regulation.

The Wolfsberg statement recognises that there is little chance that account monitoring will be able to identify individual transactions linked to specific terrorist attacks, but it emphasises the importance of continuing to look for and report suspicious transactions on the grounds that such information could provide leads for intelligence services. In particular, it highlights the need to scrutinise more rigorously the account activities of any customer involved with business sectors known to be a conduit for terrorist funds, and the need for banks to try to spot patterns and trends in terrorist financing.

Unusual/purposeless transactions

As well as monitoring the various higher-risk categories of business outlined above, the World Bank/IMF guidelines emphasise the need for financial institutions to be alert, across the spectrum of their customer accounts, to any complex, unusually large transactions, and to unusual patterns of transactions without any obvious lawful purpose.

They are instructed to look more closely at such transactions to establish as far as they can what is going on and why, and to keep a record of their findings. If they cannot obtain the information they want, or if their findings leave them still suspicious, they should consider turning the business away and, if necessary, filing an STR.

Just as some kinds of financial services products are more likely than others to be exploited for illicit ends, so financial institutions are also expected to take a view on the likelihood that particular types of customer will pose a higher risk of involvement in criminal activity (including terrorist financing activity), and to adjust their due diligence, KYC and monitoring efforts accordingly.

Politically Exposed Persons (PEPs)

Among the categories identified by FATF, increased due diligence with regard to money laundering would be expected in the case of accounts for PEPs (senior people in prominent public positions and their families or close associates). Bank staff would be expected to identify the PEP and their sources of wealth and funds; any new account in the PEP's name would have to be approved at senior management level, and more rigorous monitoring of the account would be required.

However, as the World Bank/IMF notes observe, 'Actually finding out whether a customer is a PEP is often the biggest challenge for a financial institution.' There is no official list of world PEPs to consult, for example, though 'rich lists' and other compilations are produced and updated commercially.

As mentioned above, the identification of PEPs can be assisted by an organisation's use of lists from external vendors.

Business through intermediaries

Another potentially troublesome scenario involves clients introduced to financial institutions by intermediaries or other third parties, when the financial institution itself does not carry out the usual customer due diligence. In such instances, the IMF/World Bank guidance recommends that banks should make sure that the agent who brought the new business is obliged by the relevant regulator in the agent's home country to perform customer due diligence, that they have in fact collected sufficient information about the customer in question, and that the information can be made available promptly if it is required.

Financial institutions need to be particularly careful when business is introduced to them by an agent based in another country. According to the IMF/World Bank commentary:

> **'Several countries . . . require that the introducer should be an individual or an institution that is subject to AML controls, is supervised by a regulatory body with responsibility for compliance with AML controls, and is located in a country that complies with FATF standards.'**

Source: Schott, P.A. (2003) *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism,* World Bank/IMF, Chapter VI.

Customers from high-risk geographic locations

It is most important for financial institutions to be able to identify customers and transactions coming from high-risk parts of the world. They should exercise heightened caution dealing with countries branded by FATF as higher risk in the fight against money laundering and with countries in which there is terrorist-inspired conflict or where those who support such conflicts raise funds. Determining which countries pose a heightened risk should again be clear. Other than FATF, there are lists from Transparency International (related to bribery and corruption – the CPI Index) as well as the Basel AML Index. Each organisation should set out how it will determine its list of high-risk countries. Transactions with such countries are not necessarily prohibited, but they are considered to carry higher risks and should be scrutinised accordingly. Again, if a bank has any doubts that a transaction with such a country is above board, it should think about declining the business and also consider filing an STR under its suspicion-reporting obligations. Additionally, the national security or regulatory authorities may have identified specific jurisdictions as being of particular concern, as may the management of the financial institution itself, if it has effective procedures in place for tracking the release of such information.
Banks and other financial institutions should also bear in mind that as the global marketplace becomes increasingly interconnected, it may become necessary to extend greater due diligence practices to other groups beyond their direct customers, particularly if there are higher-than-average risks attached to the relationship. These groups might include, for example, customer employees, other parties to trade transactions, correspondent banks as well as agents and suppliers working for their customers.

Charities and NPOs

Charities and non-profit organisations (NPOs) may be open to abuse by terrorist groups, often by diverting funds originally raised for humanitarian purposes. It is therefore crucial that financial institutions should carry out enhanced due diligence to ensure that they ‘know their charity’.

Senior management should approve any new relationship, and should bear in mind that there could be high risk attached to the business. A bank representative should visit the charity premises, meet the leaders and prepare a report on the visit, including such details as:

- the organisation's legal type and the activities for which it is licensed, its sources of capital, the number of staff employed, number of years established at the present and previous addresses, the nature of its present activities and its geographical location
- personal details for the directors/owners, and information about their powers
- any involvement of a PEP
- typical size and sources of donations
- whether the charity is licensed to receive donations locally or overseas.

Financial institutions with charitable or NPO customers also need to monitor their accounts closely, and to be aware of potential red flags, such as the following:

- corporate layering or 'routing' – transfers between the charity's bank account and those of its directors or staff for no clear reason
- wire transfers by charities or NPOs to beneficiaries based in countries known to be bank or tax havens, or countries of concern for terrorism purposes
- lack of apparent fundraising activity (in other words, a lack of small cheques and small internet or other typical donations) that would normally be connected with charitable bank deposits
- transactions with no logical economic purpose (e.g. no link between the activity of the charitable organisation and other parties involved in the transaction).

Voluntary best practice guidance for charities issued by the US Department of the Treasury is also worth mentioning. This guidance includes a section on financial accountability and practices which may impact on charities' dealings with financial institutions holding their accounts, at least insofar as it shapes the typical NPO account activities and profile that a bank with charitable accounts might expect to see. These guidelines state that:

- The charity should have an annual budget, overseen by the board.
- There should be one individual appointed as the finance officer, with responsibility for day-to-day control over the charity's assets.
- Charities with annual gross income over a $250,000 limit should bring in an independent accounting firm to audit the accounts and produce a financial statement each year.
- Full records of all money received and spent (including salaries and expenses both domestic and international) should be kept by the charity, with details of every charitable disbursement including the name of the recipient, the sum given and the date.
- As soon as money received has been recorded, it should be deposited in the charity's bank account.
- Cash in particular should be paid in promptly.
- If possible, money to be disbursed should be sent by cheque or via a wire transfer rather than in currency.
- When the money is going to areas without normal financial services and there is no option but to send currency, funds should be provided in smaller increments for short-term needs, rather than large lump sums for longer periods.
- The charity should also keep detailed records of such currency payments.

IT SYSTEMS

IT systems can be expensive and AML/CFT systems are no exception. Particularly in an emerging markets environment where valuable corporate money is already being spent on policies, procedures, personnel and training, the temptation may be to skimp on systems expenditure. This is a mistake. It is almost impossible to comply with international best practice unless you have some minimum capability to do certain key things and systems are now effectively an essential part of your organisation's capability to do this. Set out below are different types of systems plus their capabilities and ideas on how Compliance departments can get 'smart' information on constrained budgets.

Name check portals/filter systems

These are systems that will screen the names of customers against regularly updated lists of prohibited persons, in order to comply with the international requirements referred to earlier. There are various subscription products (such as Thomson Reuters Worldcheck or Mimiro) to which financial organisations subscribe. (It is owned by Thomas Reuters, but is still called World Check.) Names of proposed customers are input to the system, either manually or automatically (see 'Combined systems' later on) and the system then compares the name with a composite list of various proscribed persons, typically drawn from the United Nations list, the US OFAC (Office of Foreign Asset Control) list and any national list in force in the country where the financial organisation is located. If there is a name match the system produces a report which can then be investigated in the manner described earlier. As mentioned earlier, such systems are also used for determining whether or not a customer is a PEP (and also for adverse media if required), and hence whether enhanced due diligence should apply to them. They are also used by financial institutions to sweep the entire customer base periodically to check that existing customers have not become either proscribed or politically exposed during the interim period.

Transaction Surveillance systems

The function of these types of systems is to detect transaction patterns or individual transactions which are unusual through a set of 'rules-based' scenarios (often referred to as detection scenarios). Information describing expected account habits is input into the system at the start of the relationship. Categories of information typically cover such items as expected account turnover, expected largest single payment, expected largest cash payment, identities of major customers and suppliers and their banks and countries of operation, expected highest monthly balance, etc. This information is obtained from the customers themselves. The system then monitors the accounts for transactions or patterns of transactions which fall outside the expected profile contained within the system through the set detection scenarios, and produces an exception report if there is a variance above a given range, which can be specified by those running the system (e.g. exception reports to be produced at variances greater than 30 per cent,

40 per cent, 50 per cent, etc.). In practical terms, the challenge for Compliance Officers is always the same: namely, which detection scenarios to apply (and to what customers) and to set the variance levels at rates which are not so high as to produce no exception reports at all, and yet which are not so low as to produce hundreds or even thousands of reports, which then have no prospect of being analysed for potential suspicious activity, as described in the example below

Example

In the first decade of the 21st century, many US financial firms faced Example fines and regulatory sanctions from the Federal Reserve Bank and other regulators for failing to implement transaction monitoring systems correctly. It had become a requirement that banks should implement such systems, but a problem was that having done so, the banks were not prepared in terms of staffing and skill sets to analyse the exception reports produced by the systems. In one instance, a reputable international bank's New York office had installed a transaction monitoring system which was producing many hundreds of exception reports. However, only one person was available to review and analyse the reports and that person had many other responsibilities.

It follows that such systems can also be used for the purposes of mandatory reporting, should regulations require it. The mandatory reporting thresholds or transaction descriptions are input into the system, which then recognises transactions above the thresholds that then need to be reported to the national financial intelligence unit, whether manually or automatically, direct from system to system.

Beyond the simpler, rule-based systems described above, it is possible to purchase so called 'intelligent' systems that use 'fuzzy logic' and databases drawn from very wide pools of customer data to predict account behaviour patterns for certain classes of customer. For example, in circumstances

where transactions have occurred on an account which do not fall outside the set parameters within the rule-based system (and which, hence, will not produce an exception report) an intelligent system will be able to detect that, nevertheless, whatever the customer has told you to expect, this particular transaction pattern is unusual for other customers of that type. (For more information, see the sections on the uses of AI later in this chapter.)

Combined systems

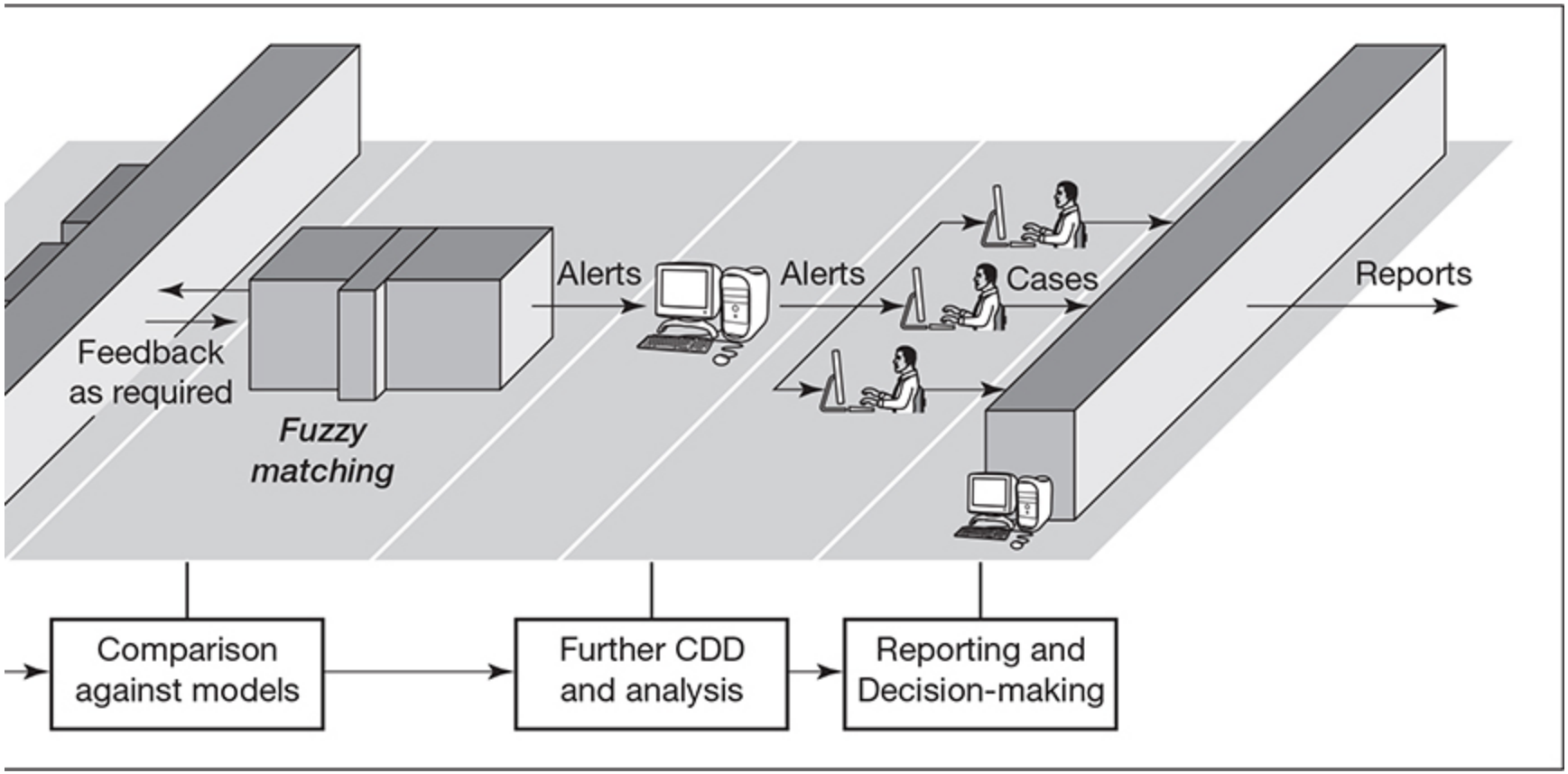
The largest institutions will have global systems which combine all the different capabilities described above in one all-encompassing package which is linked to the organisation's main banking system and which has been specifically tailored to the organisation's own anti-money laundering policy. These combined systems can cost many scores of millions of dollars and provide a complete system solution for client screening, blacklist checks, new customer acceptance and onboarding, risk-rating, transaction monitoring, mandatory reporting, exception reporting, records retrieval, transaction blocking and account freezing.

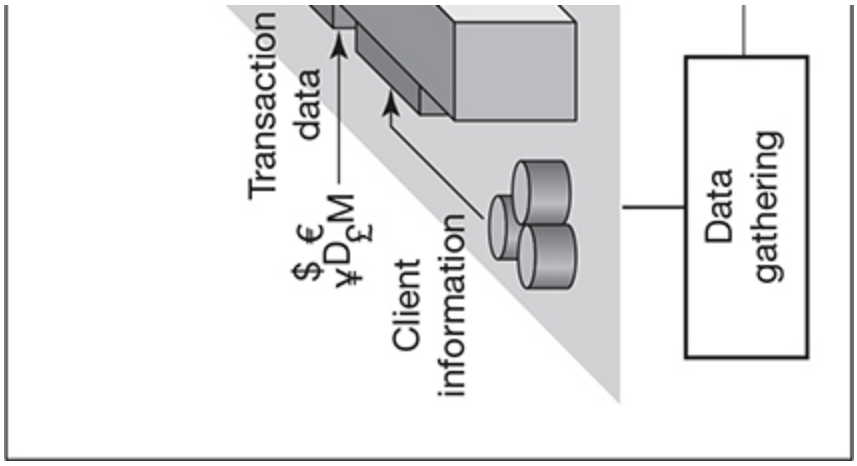
Figure 3.3 shows an intelligent transaction monitoring system. Figure 3.4 shows a process flow for a combined system capable of accepting or rejecting new clients and allocating different intensities of monitoring activity in accordance with a risk-based approach.

Spending many millions of dollars on AML/CFT systems may still be well outside the budgetary constraints of many developing countries' financial institutions. This means, therefore, that AML/CFT Compliance Officers in those countries must often seek to do the best they can with what is available, identifying the highest-risk areas and concentrating on those while also seeking and fighting for additional resources at opportune times.

A particularly high-risk area is that of proscribed persons – the terrorist lists. As a financial institution grows it becomes impossible to accomplish name screening effectively without a system and this is, therefore, the essential place to start. A simple, limited user subscription to one of the available databases will provide a level of protection against taking on or retaining clients on proscribed lists and will also assist in identifying potentially higher-risk clients such as PEPs.

Figure 3.3 **An ‘intelligent’ AML system**


Feedback
as required
Fuzzy
matching
Alerts
Alerts
Cases
Reports
Comparison
against models
Further CDD
and analysis
Reporting and
Decision-making

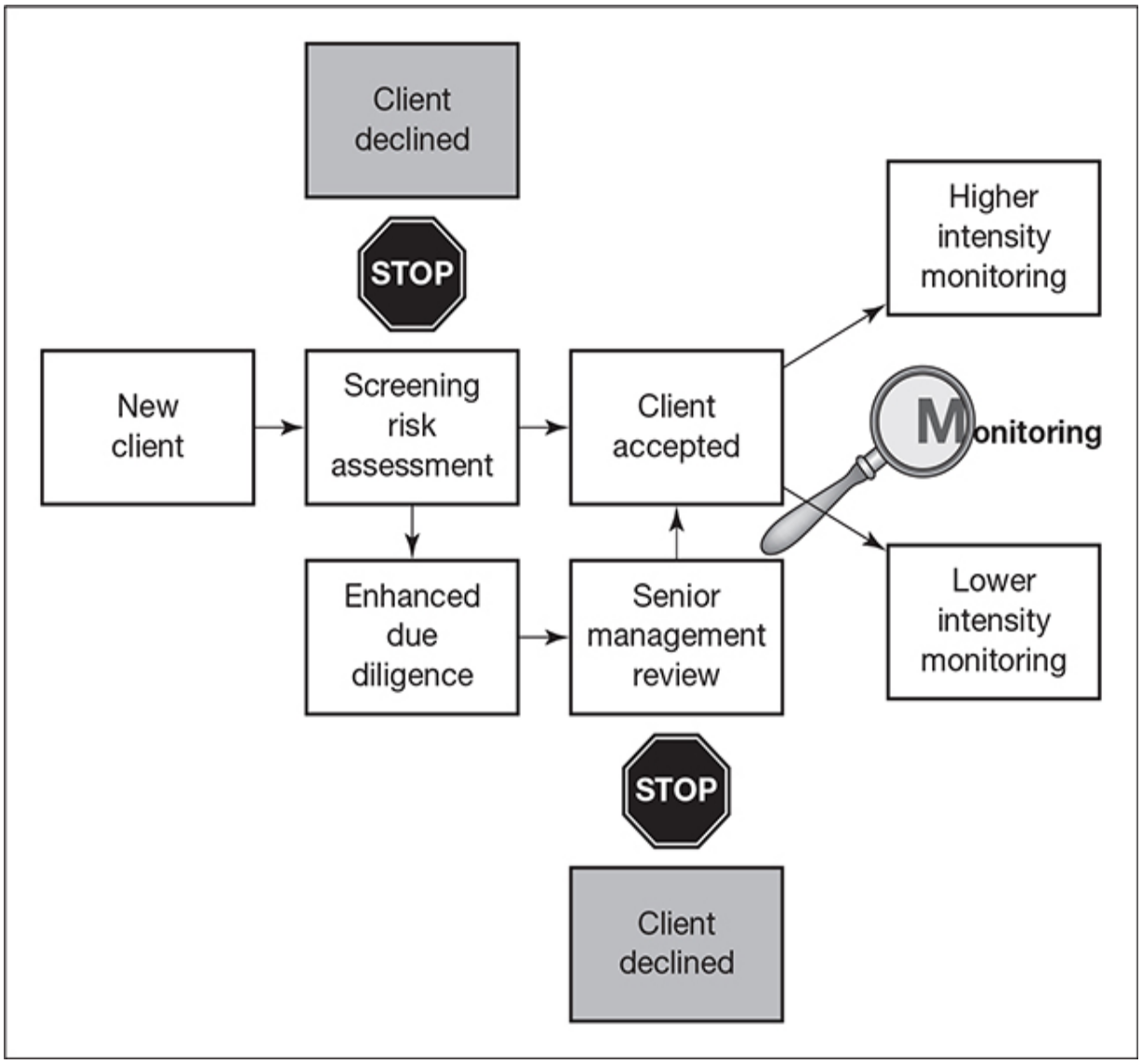


If the organisation's core banking system is already handling mandatory reporting requirements, then a discussion with the IT department ought to enable a Compliance Officer to access additional information which is relevant. For example, again using a risk-based approach, it ought to be possible for a Compliance Officer to data-mine the core banking system for the following types of relevant information:

- large transactions
- daily account opening
- turnover reports
- foreign currency remittances above a certain amount, in and out
- remittances to and from countries of money laundering or terrorist financing concern.

By accessing such information from the organisation's core banking system, a Compliance Officer can also learn a lot about the money laundering and terrorist financing risk profile which the various businesses are assuming in practice.

Figure 3.4 **Client acceptance process flow**



THE USE OF ARTIFICIAL INTELLIGENCE

The application of Artificial Intelligence (AI) and machine learning technology to the fight against financial crime is in its infancy, yet we are seeing its deployment to good effect in a number of key areas depicted in Figure 3.5 and this will likely expand over the next few years. It will also progress beyond the largest financial institutions which are incorporating AI

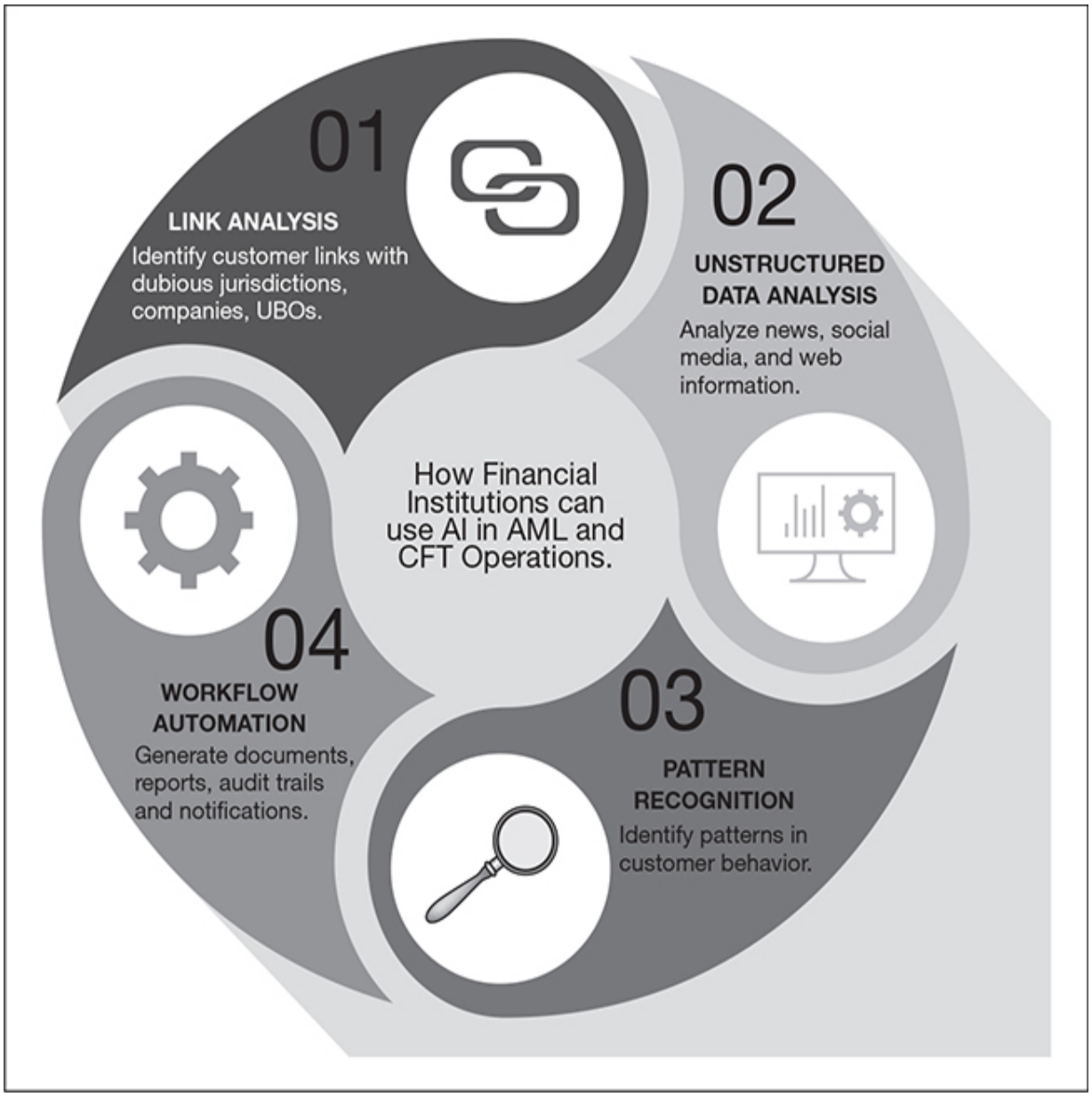
now and will become mainstream, as happened with other technology solutions such as the threshold-based systems described above.
AI is defined in the Merriam-Webster dictionary as

> ***the capability of a machine to imitate intelligent human behavior***

and machine learning is defined

> ***the process by which a computer is able to improve its own performance (as in analyzing image files) by continuously incorporating new data into an existing statistical model.***

Figure 3.5 **Uses of Artificial Intelligence in AML and CFT operations. From https://www.trulioo.com/blog/ai-enhance-due-diligence/**



Customer Due Diligence (CDD) and transaction surveillance are two areas where the application of AI and machine learning is not futuristic, but current.

Application of AI in the CDD process

In order to comply with the law, financial organisations are employing increasing numbers of CDD specialists to read what the relationship managers or the customers themselves have written on the CDD forms and sort out errors and conduct basic research. Customer onboarding has

become a paper-heavy, expensive, manual process, which is costing more and more each year. What AI systems can now do is start to take on some of this work. For example:

- A human analyst might check for reports of financial irregularities on the charity commission website; or check for evidence of operating as a phoenix company; or that a solicitor is registered at the law society. All of these checks can be performed reliably by an AI system in a short space of time.
- AI can read an application form and decide whether statements given are plausible. Does it really add up that a takeaway restaurant in a back street in a provincial town has an annual revenue of £10m?
- When an address is given for a business that, say, would typically require warehousing transportation facilities, AI can search Google Earth for the address, look at the picture and determine whether or not it looks as it should or whether, for example, it is in fact a residential address.
- AI can search public sources from the internet and official websites for information and documentation on address, incorporation, directors, ownership and business activities. It can curate and read that information and indicate whether or not it is accurate or sufficient.

Application of AI in transaction surveillance

An existing problem with current suspicion recognition software is the high rates of ‘false positives’, often well up into the 90 per cent bracket as a percentage of all transactions flagged by the system being used. This leads to a waste of (expensive) human resources in analysing and discarding those alerts. To counter this, some banks have been initially experimenting with and then implementing machine learning systems that can assist in reducing the false positive rate and also self-generate new money laundering scenarios to test against, based upon large data sets. Such solutions involve using data gathering, ‘clustering’, segmentation and classification to build a knowledge base about a customer. Each transaction is then watched for its frequency and the quantum of funds involved in those transactions, to build learned models of what constitutes suspicious activity.

Another use of AI in the world of combating financial crime has been the use of a specialised form of 'chatbot' called an 'auditbot' (an AI programme that wanders through the applications and programmes that particular categories of staff are using, engaging with them and asking them audit-type questions about what they are doing, how and why they are doing it, and what results they are seeing. It is now very likely, if not inevitable, that the development and use of AI will radically transform the way in which financial institutions are managing financial crime risk, perhaps in ways that no-one has yet thought of.

TRAINING, COMMUNICATION AND AWARENESS

Training is an essential component of the Compliance Officer's role. Unfortunately, it is also something that tends to be ignored when more pressing operational requirements weigh in upon the Compliance Officer. Such an outcome should be avoided at all costs since not only is training a regulatory requirement in all compliant countries, it also helps to generate the culture of awareness among staff which is such an important part of the organisation's overall AML/CFT effort. It is unlikely that you will be able to train everybody in everything which you want them to be trained in, immediately. It is more likely that, with limited resources, you will have to prioritise. In order to prioritise you need to be able to assess the most important requirements and then select accordingly. To do this, you will need to conduct a Training Needs Analysis (TNA).

Training Needs Analysis (TNA)

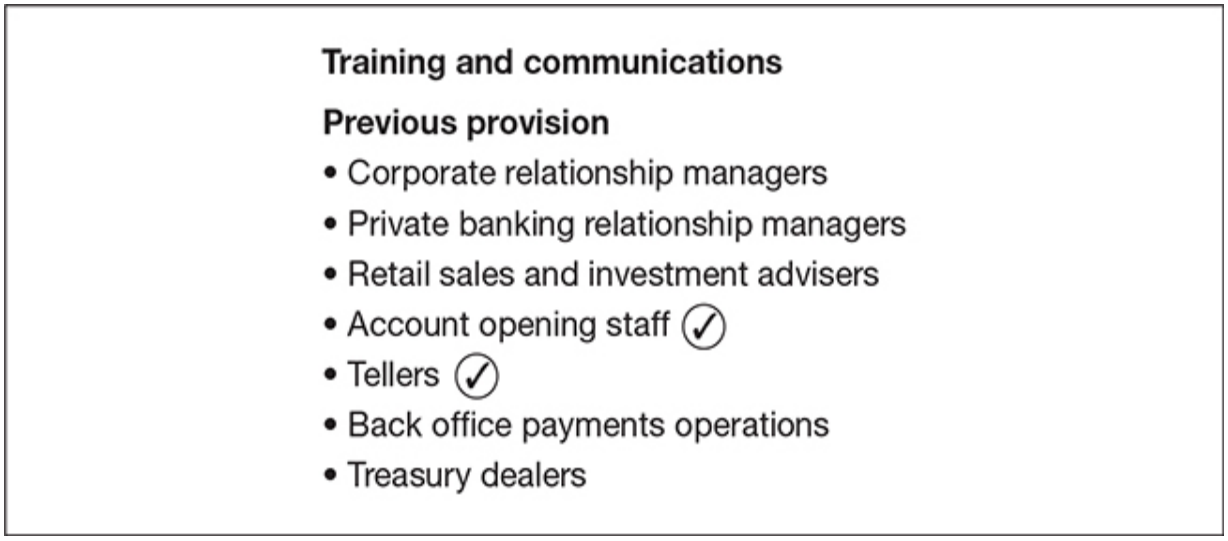
What is a TNA? It is a simple, logical system used by training and development professionals to enable training needs to be established within an organisation and thereafter to set priorities. The processes are outlined below:

Stage 1 – Establish previous provision

The first stage of a TNA is to work out what training has already been done in the organisation within a given period (e.g. the past two years). Relevant questions are:

- How long ago was the training done?
- To whom was it given (e.g. which businesses, which job roles within those businesses)?
- What was the content?

Figure 3.6 **Previous training provision**


Training and communications
Previous provision
• Corporate relationship managers
• Private banking relationship managers
• Retail sales and investment advisers
• Account opening staff ✓
• Tellers ✓
• Back office payments operations
• Treasury dealers

For example, look at the information on previous training provision across business and job functions shown in Figure 3.6.
Of all the jobs listed across the businesses shown in Figure 3.6, you might find that the only training which has been done is for account opening staff and bank tellers; those dealing with account opening documentation requirements and mandatory cash reporting thresholds, respectively. This would mean that no other training had been provided for any of the other job descriptions.

Stage 2 – Establish current and future requirements

Having worked out what training has been done and for whom, it is now necessary to establish what training needs to be done going forward. This entails a degree of enquiry by the Compliance Officer. What training is

required by the law of the country? Have there been any poor internal or external inspection reports within specific business areas which are indicative of a training need?
Are there any upcoming reviews or inspections (e.g. a central bank inspection or a review by a correspondent bank)? Are there any particular business risks which have raised their profiles recently? Does the - organisation's own AML policy require certain types of training, and if so in what? Have there been any disasters or 'near misses', indicating that further training needs to happen (e.g. nearly opening an account for someone on a terrorist list)?

Stage 3 – Establish the gaps in provision and prioritise

Having worked out what training has already been done and having established what training *needs* to be done, the Compliance Officer should now be in a position to map the existing provision against the current and future needs in order to arrive at a list of training requirements. But this on its own will not be enough. Unless the Compliance Officer is blessed with enormous resources, there will simply not be the time, people or money to achieve everything which needs to be achieved straight away. Therefore, the Compliance Officer will need to prioritise and create a training schedule accordingly. Here, it is better to be realistic rather than overambitious, and it is absolutely necessary to have very clear training objectives with 'do by' dates attached to them. For example, referring back to Figure 3.6, the Compliance Officer in that organisation might decide that they need to address the most basic requirements first, while also ensuring that their current highest business risk is also covered. They might therefore decide on the following training prioritisation:

By 30 June 2020:

- all staff to have received 'basic training'
- 100 per cent record in induction training
- all payments staff to have received specialist training on suspicion indicators in funds transfers.

Risk-based approach to training

This is a risk-based approach to AML/CFT compliance training. It demonstrates to regulators, potential overseas correspondents and stakeholders generally that the AML/CFT Compliance function is organising its training carefully, thinking about the issues and creating prioritised training to address the key risks. Training to address less-important perceived risks can then follow. The important thing is for the Compliance Officer to be able to show not only that they are undertaking training, but also that they are targeting the training efforts to make them as effective as possible when matched against the risks which the organisation is confronting.

Wide approach to training

There is a temptation to think that training only counts if it is people sitting in a classroom listening to a person (e.g. the Compliance Officer) talking and showing slides. This is too narrow an interpretation of the activity. The wider phrase 'training and awareness' encompasses any method used to convey knowledge, teach new skills, change attitudes and encourage staff to do what is required.
Beyond classroom training, an organisation's AML/CFT training programme is limited only by resources and need. Below are some of the other methods that can be deployed:

- e-learning – the use of web-based learning and knowledge testing applications accessed via users' PCs and tablets
- self-study – the distribution of books, notes and pamphlets for people to read in their own time
- videos – hard-hitting and informative DVDs or online videos dealing, for example, with relevant law and the methodologies used by money launderers and terrorist financiers
- poster campaigns – posters can be sited at key locations (e.g. by lifts or water coolers) containing key messages, for example in relation to KYC
- email campaigns can be run over several weeks or even months, with each email prepared in advance and designed to deliver key messages

- online tools and virtual assistants that prompt staff with tips and guidance during key processes, such as onboarding new clients.

Sometimes organisations may not just wish to train their staff, but to prove to the outside world that those staff have achieved a certain standard of knowledge and competence. They may therefore wish to obtain independent accreditation for the learning achieved with a certificate that counts as more than a certificate of attendance, typically after the passing of some exam.

The largest global financial institutions will tend to adopt a blended approach to AML/CFT training, mixing classroom with distance learning techniques (techniques in which the learner is not physically present with the teacher in a classroom). E-learning tends to play an important role, given the need to train large numbers of people in the same way across vast distances. Such systems will often have self-certification built in, i.e. the user takes a test and if successful, the system produces a certificate confirming that they have passed the test, which is then centrally recorded by the system. Systems of this type can also be constructed as a series of discrete 'chapters' or 'modules' which are relevant to different people in different businesses and/or in different countries and using different languages. The most advanced systems are sophisticated in this respect and consequently quite expensive, although the per person training cost over time can be greatly reduced. An example is shown in Figure 3.7.

The training requirements of the AML/CFT staff should also be taken seriously to ensure they are up to date with all regulatory, legal requirements as well as 'best practice'.

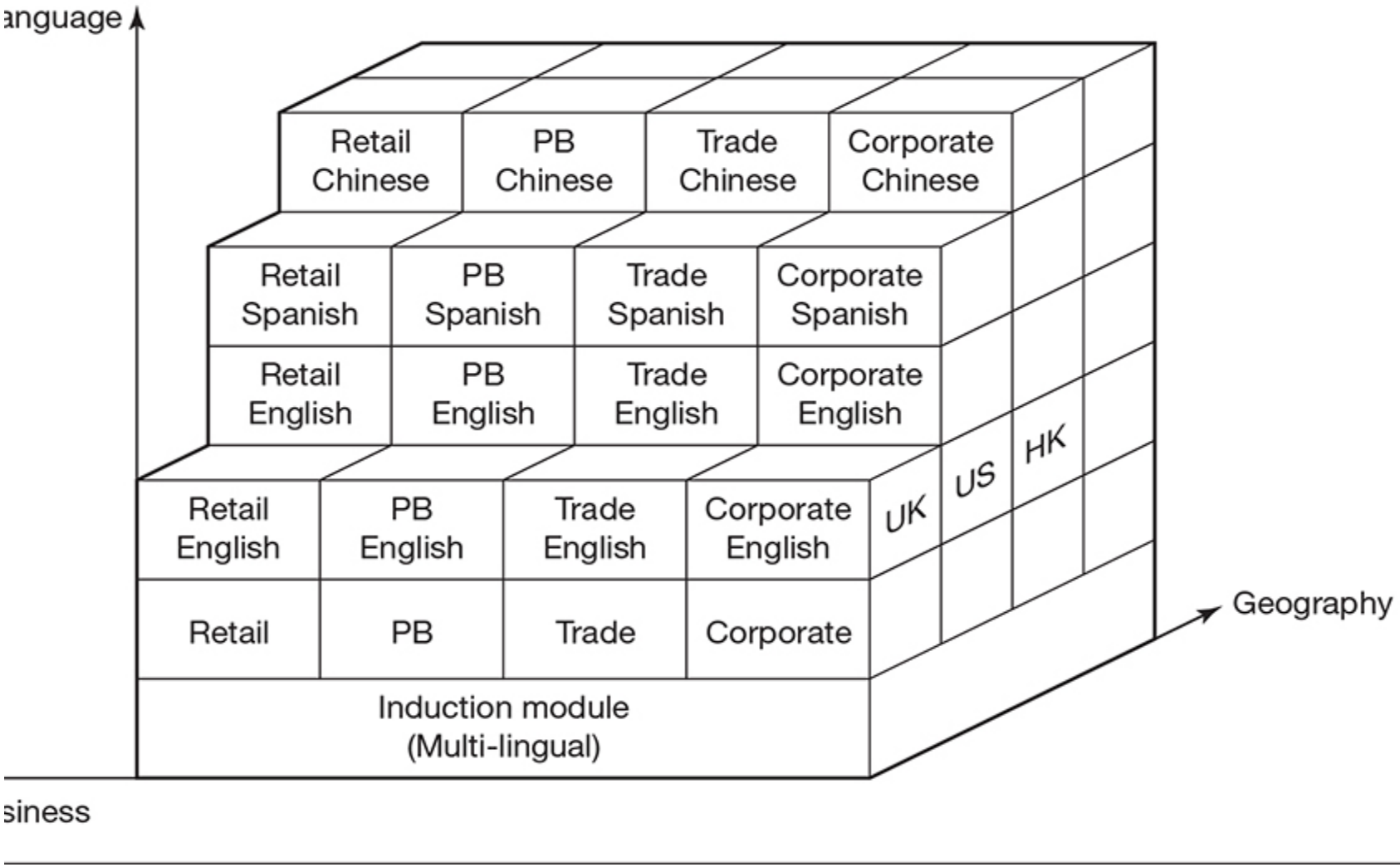
Finally, it is important that accurate records of training are maintained and recorded, what training (the material), who exactly received it and when.

A word about CFT training

To many Compliance Officers, the idea of training staff in CFT is a difficult concept to grasp. After all, what on earth can you train people on? Everybody knows by now that, without a tip-off from the security services, terrorist financing is very very hard to detect. Not much can enhance an organisation's capability to detect sub-$10,000 transactions when they are within the normal transactional range on the account or relationship in question, and when there are no other features marking them out as

'suspicious'. Tie this in with other known truths concerning source of funds or source of wealth (which are not necessarily criminal where terrorist financing is concerned) and the need to keep records readily available for when the security services come calling (essential), and, so the argument goes, training on CFT can be confined to the following points, inserted succinctly at a time or place of your choosing within an existing AML programme:

Figure 3.7 **E-learning training concept**


anguage
Retail Chinese
PB Chinese
Trade Chinese
Corporate Chinese
Retail Spanish
PB Spanish
Trade Spanish
Corporate Spanish
Retail English
PB English
Trade English
Corporate English
Retail English
PB English
Trade English
Corporate English
UK
US
HK
Retail
PB
Trade
Corporate
Induction module (Multi-lingual)
Geography
siness

E-learning training concept
×3 Dimensions. . .
Business – provides business-specific material
Geography – provides relevant local legal and regulatory content
Language – provides content in multiple languages

- Terrorist financing is like money laundering, except it's often in reverse, i.e. using legally derived funds for an illegal purpose.
- The amounts used to fund terrorist attacks are too small to make traditional AML tools much use, so all efforts should focus on effective customer identification, efficient name-screening, excellent record-keeping and unfailing cooperation with law enforcement in the investigation of suspects and their accounts.
- And . . . that's it.

If the above is essentially what your CFT training says – and if that is pretty much all it says – then you could be selling the risk short within the overall context of your AML or wider financial crime training programme. Why? First, because training on CFT should take place within the context of a discussion about terrorist financing, *not* one on money laundering. Though they share many of the same characteristics, the two are essentially different activities undertaken by different people for very different purposes. A failure to recognise this and provide appropriate treatment to terrorist financing within the overall AML/CFT programme risks a charge that you have conducted 'by-the-way' training (as in 'Oh, and by the way. . . ') and failed to educate staff at a basic level.

Second, suspicion recognition training for terrorist financing isn't the total non-starter which it may at first seem, especially if you distinguish between the financing of terrorist movements generally (what we may refer to as

Type I terrorist financing) and the funding of individual attacks (*Type II*). It is of course true that, given the relatively modest amounts required to fund individual attacks, systems and people are unlikely to detect specific funds and fund movements earmarked for those attacks. But fund-raising activities further back up the chain have detectable characteristics that staff need to be made aware of so that they can identify them and take appropriate action.

Third, while some might say that a good 'test question' for the CFT elements of the overall AML/CFT training programme should be '*Are there any suspicion indicators that are exclusive to terrorist financing which staff wouldn't otherwise be aware of from the AML part of the programme?*', this is too restrictive an approach and moreover is definitely not the approach which would have been adopted had money laundering and terrorist financing both arrived as issues on the financial services scene at the same time (instead of money laundering coming along first.) Rather, what organisations should be doing for *both* subjects is providing ongoing training which, apart from the legal basics, is rich in case study, example and explanation, and which *over time*, enables the relevant workforce to construct internal reference frameworks for a wide range of situations and their potential causes; situations which they can compare with events and information that they encounter in their daily work. A workforce that has been educated in this way will be familiar with the underlying methodologies, preferences and structures of both non-terrorist and terrorist criminal groups and is likely to offer the organisation better levels of overall AML/CFT compliance and protection.

Designing and structuring the CFT elements of the AML/CFT training programme: training review

As with anything else, training should be geared around the risks that the organisation faces. If you are concerned that your existing training programme may not be hitting the mark as far as CFT is concerned, perhaps because it had been inserted by a predecessor as an 'add on' to an existing (and maybe longstanding) AML training programme, or because you do not think that it is detailed enough, then you should conduct a training review. Not only will this help you frame the relevant programme content, it will

also help demonstrate that your training has been constructed intelligently, and not just thrown together to tick a box on an internal auditor's checklist. A training review is, in essence, no different from a Training Needs Analysis (TNA) in that its purpose is to assess actual versus required training provision, to link training needs to specific individuals (e.g. on a role or business basis) and to set priorities. Remember, the basic structure of a TNA is designed to answer a series of questions about your organisation's training, and to plan further training accordingly:

- Establish current provision levels. (What training has been/is being done? To whom? Covering what?)
- Establish the organisation's needs. (What are the areas of highest business/product/country risk? What are the legal/regulatory requirements? What corporate events have taken place (e.g. key personnel changes, business acquisitions, regulatory or operational 'near misses', etc.) which raise the risk profile?)
- Map the needs against the provision to produce a training plan.

Ideally, the training review should occur as an integral part of the wider, regular business risk review, although if it has been omitted from that process it should still be undertaken. The training plan should, of course, be specific about who is going to be trained, what the training will cover and the desired outcomes (e.g. enhanced awareness of use of wire transfer networks by payments staff; or enhanced awareness of use of opaque structures and agent-consultants by corporate and private banking relationship managers, etc.).

Contents of a CFT training programme

Based upon the results of the exercise described above, different organisations will end up with different conclusions about how best to segment the various potential content combinations, but it is possible to conceive of the following type of structure, accommodated as an integral yet distinct element within the wider AML training framework.

Foundation

The foundation elements of the CFT training programme would deal with the core issues of general relevance to most people who have been assessed

as requiring AML/CFT training. These issues would encompass areas such as:

- *Background* – definitions of 'terrorism' and 'terrorists', and the difficulty in reaching international agreements on this; the effects of terrorism (human, economic, political); the link between terrorism and terrorist financing; and the nature of the obligations of financial firms to combat it.
- *The legal and policy framework* – the essential elements of the international regime put in place including key base items such as: the 1999 UN Convention for the Suppression of the Financing of Terrorism; UNSCR 1373; the FATF Recommendations; and details of regional (e.g. EU) and national legal and regulatory requirements.
- *Origins of terrorist funding* – basic methodologies for collecting finance used by different terrorist groups, both current and historic (e.g. Al-Qaeda, ISIS, Provisional IRA, Tamil Tigers) involving, donations from sympathisers, collections by religious and cultural bodies, diversion of funds from legitimate charities, business takeover, fraud, organised crime, seizure and exploitation of national resources (oil, water, etc.) and so on.
- *Personal obligations and internal reporting* – linking in with AML structures, MLRO, SARs, etc.

Additional

The additional elements of the CFT programme would contain more detailed information relevant to front line, customer-facing, operations and managerial staff designed to raise their awareness of how terrorist financing is conducted and would encompass items such as:

- *Factors informing the risk assessment* – e.g. business area (conflict zones involving terrorism), customer type (charity and NPO customers with operations in conflict zones involving terrorism, trading companies, money remittance businesses, cash intensive businesses in areas of ethnicity connected with conflict zones involving terrorism), product type (wire transfers, trust and nominee accounts, off-street cash conversions and forex purchases, single premium insurance products).

■ *Detailed examples of terrorist financing: typologies and structures* – for example cases involving:

– payments and receipts unrelated to the provision of legitimate goods or services
– unusual and repetitive wire transfer activity
– charities with unusual donation profiles
– unusual signing arrangements on accounts
– account takeover of student accounts by terrorists
– credit card fraud used to fund terrorist operations
– medical insurance fraud used to fund terrorist operations
– terrorist financing through early redemption of policies
– dormant accounts
– structured payments.

Specialist/specific

The specialist/specific elements of the CFT programme would contain items of specific operational relevance to particular sections of staff conducting certain activities relevant to some important aspects of CFT operations, such as:

■ *Know Your Customer (KYC) and Customer Due Diligence (CDD)* – for staff opening accounts and checking identification, training and examples showing how the operation of watchlists enhances the importance of customer identification and verification data quality.

■ *Identity theft and fraud* – for staff opening accounts and checking identification, training and examples showing how terrorists have used identity theft to gain access to the financial system, and the enhanced importance of correct application of measures to deter and detect identity theft.

■ *Dealing with watchlist problems* – for staff conducting client acceptance checks and others involved in dealing with new business, training and examples showing how the organisation handles issues such as name matches and false positives (where a customer or potential customer's name matches that of a proscribed person, but where there is uncertainty over whether the identities actually match).

Taking such a structure as a starting point, it ought to be possible to construct powerful combinations of training that would be relevant to particular business units or job types. During the course of either a training review or a wider CFT business risk assessment, AML/CFT Compliance Officers may find that certain combinations suggest themselves, which can then be incorporated as distinct elements within the overall programme.
However such a programme is constructed, gone should be the days when CFT is the 'by the way' item at the end of your AML training.

A 'PRO-BUSINESS' APPROACH

The Compliance Officer performs one of the most critical risk control functions within the organisation – namely the safe and effective management of the analysis and reporting of unusual and/or suspicious transactions to the national authorities. They also have additional responsibilities which require a real understanding of and empathy for the businesses they serve.

General approach

Compliance Officers must approach their duties from the perspective of a commercial banker committed to the commercial success of the organisation, combined, however, with an essential objectivity and a deep commitment to preventing the use of the bank's services by criminals, and to cooperating with the national authorities in the successful investigation of actual or attempted instances of money laundering. Each of these perspectives in the overall approach is as important as the other.
Compliance Officers need to remain sensitive to the commercial objectives of the organisation, otherwise they risk creating unnecessary and counter-productive friction with the businesses they serve. They must remember that the organisation's objectives are primarily concerned with the provision of excellent services to customers at a profit. Forgetting – or even appearing to forget – that reality, makes the Compliance Officer appear detached from

the business, and reduces their credibility and effectiveness. Compliance Officers can demonstrate their alignment with business objectives by:

- showing an interest in business performance
- maintaining regular contact with business managers
- attending key business presentations and events (e.g. product launches)
- exploring, rather than dismissing, views which contradict their own
- spending 'as much time listening as talking. . . '.

In doing so, Compliance Officers are likely to learn more about the various businesses within the organisation, and thus enhance their ability to make judgements on reported transactions. In particular, the objective of any investigation is always to decide whether a transaction is suspicious and whether it has to be reported, not to prove that the Compliance Officer's initial 'gut instinct' is always correct, in all circumstances.

Equally, Compliance Officers must be wary of accepting explanations for transactions from business managers or customers which are objectively unconvincing and which are unlikely to withstand detailed scrutiny. They must have the strength of character and the determination to challenge such explanations, and to dig deeper in search of the truth. At times, Compliance Officers may find themselves subjected to great pressure – particularly where a customer is a good source of revenue for the organisation – to adopt a less searching attitude towards that customer's transactions. They must resist such pressure, retaining the essential objectivity and independence which is so essential for their role.

In conjunction with the CEO, Compliance Officers should do their utmost to ensure that businesses and business managers adopt due responsibility for assessing the suitability of customers and proposed account purposes at the time when accounts are opened, discussing any uncertainties with the Compliance Officer before account opening takes place. Otherwise, a mentality can develop in which businesses see their role solely in terms of bringing business into the bank and maximising revenue from the account, rather than accepting a joint responsibility with risk functions such as compliance for the overall quality of the bank's business. Disengagement by businesses from this task can result in a wastage of resources as Compliance Officers spend their time investigating transactions that should

have been refused upfront. In the worst cases, the reputation of the bank is placed at risk as suspect business which should have been prevented at source is allowed into the bank.

MANAGEMENT OF INTERNAL SUSPICION REPORTING

For audit purposes the Compliance Officer should adopt effective procedures for the management of internal reporting of suspicious and/or unusual transactions. Three files should be maintained:

1. 'Suspicious Transactions – Initial Reports' (File 1)
2. 'Suspicious Transactions – No Action Taken' (File 2)
3. 'Suspicious Transactions – Reports Made to Authorities'. (File 3)

File 1 is the ongoing operational file containing reports that have been made by the businesses and that are being investigated prior to a decision being made on whether they warrant the filing of an external report (and for which there should be clear time limits). Following the making of a decision on external reporting, File 2 is the repository file for those cases in which the Compliance Officer decides that the transactions in question are not suspicious, and that no external report is required. File 3 is the file containing those cases in which reports are filed with the relevant authorities.

In each case following the making of a report by a member of staff, a written record must be kept of the further investigations conducted by the Compliance Officer and of the reasons behind the decision either to report externally or not to report, as the case may be. The purpose of this system is to achieve full, auditable transparency regarding the reporting and decision-making process. It is particularly important that the reasons for any decision *not* to report a case to the relevant authorities are clear and fully documented, so as to avoid any justifiable criticism of the organisation's actions in not filing such a report.

Compliance Officers should periodically remind staff about the importance of reporting unusual or suspicious transactions, and should take steps to facilitate such reporting, such as the provision of standard suspicious transaction reporting forms.

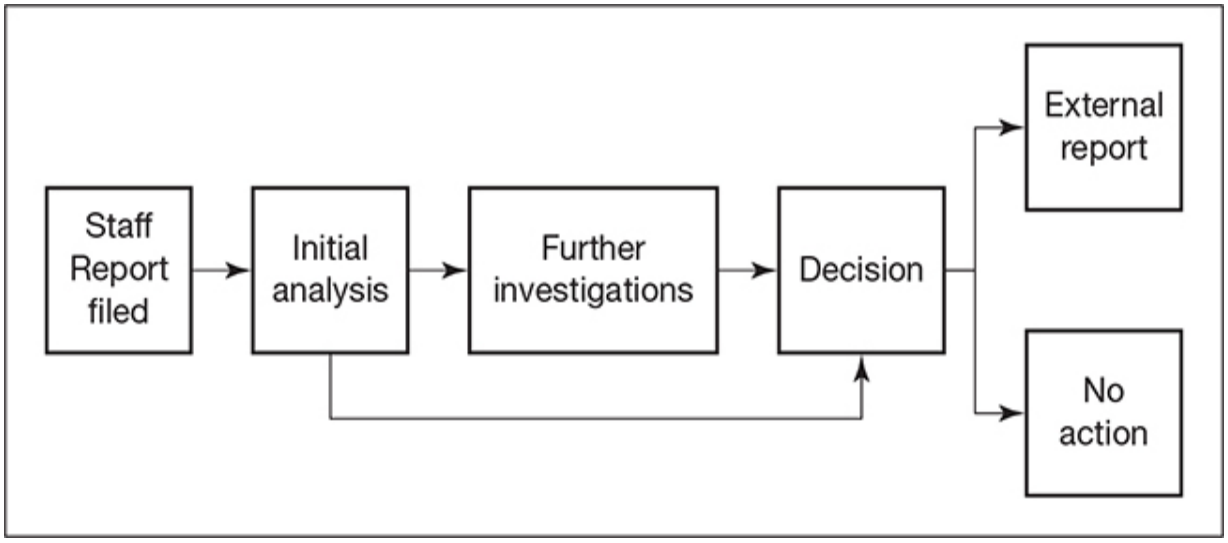
Once a report has been filed by a staff member, the procedure for the investigation and subsequent reporting and filing is as shown in Figure 3.8.

For cases in which a decision to report is made, the report itself should be submitted to the relevant authority in the format (if any) prescribed by such authority, and a copy of it retained in File 3 'Suspicious Transactions – Reports Made to Authorities'. A copy of the report should also be sent to the CEO and the customer's file should be removed from the five-year document destruction cycle, so as to prevent key historic transactional information being automatically destroyed.

Complete records of investigations leading to a decision (whether to report or not to report) must be maintained, including details of:

- staff members and any other persons spoken to, and the outcome of interviews/conversations
- documents reviewed
- explanations offered or discovered in respect of the reported transaction or transactions.

Figure 3.8 **STR investigation process**



Full correspondence records with the relevant authorities and with any other parties must be maintained following the filing of a report, along with clear records of any actions taken or permitted.
Full cooperation must be extended to the relevant authorities in relation to any investigation which they make into the reported case, including, but not limited to:

- provision of required information
- provision of required copy documents
- access to staff and premises
- liaison during regulatory visits and interviews
- access to administrative and communications facilities during visits.

Deciding whether to make a report

The critical factor in deciding whether or not an external report is required is whether or not the transaction or transactions brought to the Compliance Officer's attention are 'suspicious'. No definition of 'suspicious' can be exhaustive. In its normal everyday context, the word means 'mistrust – the imagining of something but without proof' and Compliance Officers are expected to use judgement and experience in deciding whether a transaction is suspicious or not, taking into account all the circumstances of the case. Specifically in a money laundering context, however, transactions are likely to be suspicious:
where there appears to be no convincing explanation for them, *and* where:

- they are inconsistent with the stated or apparent purpose of the customer's account; *and/or*
- they are inconsistent with the history of previous transactions on the account; *and/or*
- they are otherwise suggestive of activity known to be undertaken by money launderers.

The purpose of any initial investigation into a matter which has been reported internally is not to prove or disprove conclusively whether a suspicion is justified. Rather, it is to establish that there are no known facts

that contradict the suspicion which has been raised, or which otherwise suggest that the fears about the customer or transaction are groundless.
Chapter 6 explores the concept of suspicion in greater depth, with the use of a wide range of examples.

4

CDD, KYC and the Risk-based Approach

Background to the Risk-Based Approach

Components of the Risk-Based Approach

Mitigating controls

Regulatory environment

Special categories: Politically Exposed Persons (PEPs)

Constructing a Risk-Based Approach for your organisation

The core components of CDD

CDD processes and tools

Example risk assessment frameworks

Constructing a CDD framework for financial institutions

Constructing a CDD framework for retail/consumer banking business

Constructing a CDD framework for private banking

Excerpts from Recommendations 1 and 10 of the FATF 40 Recommendations (February 2012) and the Interpretive Note thereto:

'countries should apply a risk-based approach to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified.' (R1)

'Financial Institutions should be required to apply each of the CDD measures . . . above . . . but should determine the extent of such measures using a risk-based approach (RBA). . . ' (R10)

'There are circumstances where the risk of money laundering or terrorist financing is higher and enhanced CDD measures have to be taken. When assessing . . . money laundering and terrorist financing risks [relevant factors are] types of customers, countries or geographic areas, and particular products, services, transactions or delivery channels.' (R10 Interpretive Note)

www.fatf-gafi.org copyright © FATF/OECD. All rights reserved.

BACKGROUND TO THE RISK-BASED APPROACH

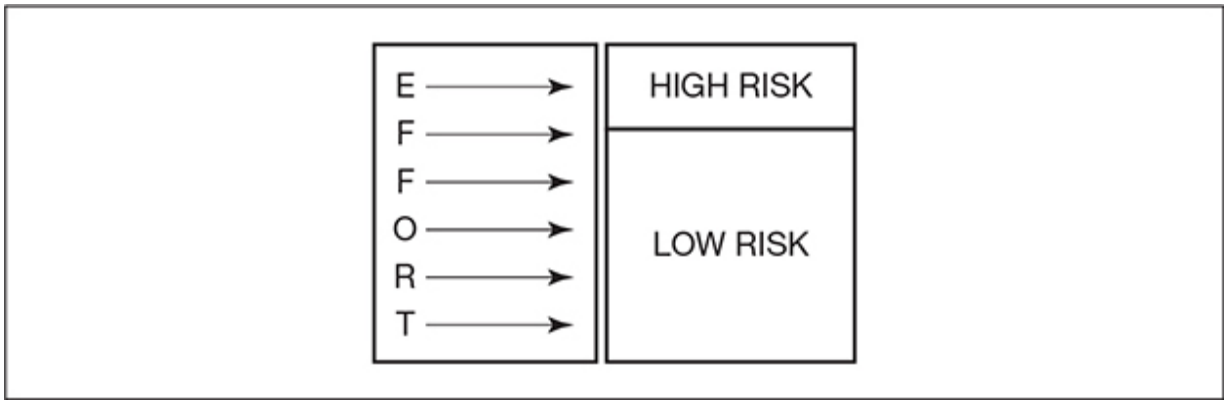
The requirement for a 'risk-based approach' generated probably the most radical overhaul in AML/CFT strategy to have been seen since the inception of global standards shortly after FATF was formed in 1989.

The so-called risk-based approach, having been initially adopted within the economically developed nations which originally formed the Financial Action Task Force (FATF) is now a general global requirement. It may be helpful for new Compliance Officers to understand not only the principles of its operation, but also its background. In doing so, they may better understand the industry and other pressures that are likely to confront the AML and CFT regimes put in place in their own countries.

Historically the various AML measures required by the original 40 - Recommendations were not welcomed with open arms by the financial - community. They were seen as bureaucratic and cumbersome, costly to - maintain, not user friendly and hostile to good customer relations. In - particular there were concerns regarding the ability of inflexible AML standards to distinguish between different types of customer, and it is this concern especially which the development of a risk-based approach has been designed to address.

For example, non-risk-based principles would require a financial institution to treat a retired state pensioner in her seventies in the same way as a businessman in his forties receiving large funds from a country known for the production of blood diamonds. That is to say that, if one did not weigh the differences between these individuals, then the same identification, due diligence Know Your Customer (KYC) and account monitoring principles would apply to both of them, even though it is clear from a risk perspective that their profiles are entirely different.

Figure 4.1 **AML: the traditional approach**

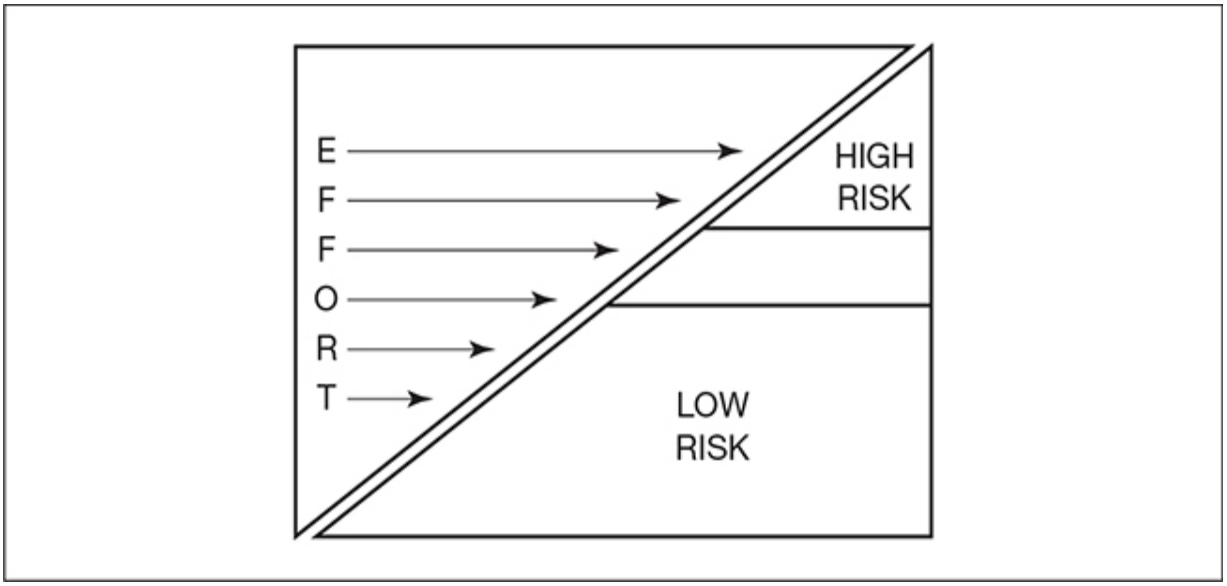


Faced with the risks, what most countries and financial institutions ended up doing was applying a 'one size fits all' approach, which was viewed as being exceedingly harsh on the vast majority of customers who actually posed very slight money laundering risks. It also meant that scarce resources were not being applied as effectively as they might be in tackling higher-risk customers and relationships. By spreading the effort equally over all customers, it was argued that 90 per cent of that effort was in effect being wasted on the 90 per cent of customers who were very unlikely to have any involvement at all with crime or money laundering, with only 10 per cent of the effort being directed at the higher risk accounts (see Figure 4.1) .

Would it not be better, so the argument went, if a risk-based system could be introduced which reversed these odds and enabled financial institutions to apply 90 per cent of their available resources towards the 10 per cent of their business which actually constituted the most serious risk? This would

mean less bureaucracy, less paperwork, less form filling and of course a more welcoming experience for most customers (see Figure 4.2) .

Figure 4.2 **AML: the risk-based approach**



It is of course the case that higher-risk customers tend to be (but are not always) wealthier, more international and worth more on an individual basis as customers. It is important to note, therefore, that from a business perspective the risk-based approach requires a considerable degree of finesse in its application to these higher-risk customers, so that they do not end up feeling that they are being discriminated against.

Pressure from the financial services industry within the developed economies led, in the early part of this century, to discussions regarding a risk-based approach. These discussions manifested themselves first as proposals and then as revised recommendations and standards. Risk-based principles have now been embodied not only in the FATF 40 Recommendations, but also in other standards and in laws and regulations such as:

- the EU Money Laundering Directives
- the revised Wolfsberg principles
- the revised standards of the Bank for International Settlements (BIS)

- the national Regulations of all EU member states
- the USA Patriot Act, as amended.

COMPONENTS OF THE RISK-BASED APPROACH

Risk indicators

How do you decide whether a customer is high or low risk from a money laundering perspective? The FATF Recommendations refer to 'customer risk factors', 'Country or geographic risk factors' and 'Product, service, transaction or delivery channel risk factors' and then go on to list some relevant factors which create 'potentially higher-risk situations'. From a practical perspective, a key requirement is a series of questions in relation to a number of important areas.

Type of customer

- Individual or business?
- High income or low income?
- Politically exposed or not?
- Introduced or brand new?
- Anomalous circumstances (e.g. geographic distance between financial institution and customer)?
- Non-resident?
- Corporate asset holding vehicle for an individual?
- Company with bearer shares or nominee shareholders?
- Complex ownership structure?

Type of business

- Which sector (industrials, trade, import/export, diamonds, arms)?
- Cash intensive?

- Does the business act solely for itself or does it represent others (e.g. investment or professional firms)?
- Type/identity of counterparties – which third parties is the customer doing business with and what is its risk profile?

Geography

- Where is the customer located (modern, developed country with advanced laws, or developing country with a developing legal system)?
- Is the customer a non-resident?
- In what other countries does the customer do business or have contacts?
- Is cash the normal medium of exchange within the country in which the customer is doing business?
- Is it a country known for the production of drugs or other high levels of criminal activity?
- Is it a country experiencing conflict or high levels of terrorist activity or insurgency?
- Is the country subject to sanctions or identified by credible sources as providing funding or support for terrorist activities?

Type of product and distribution channel

- What products is the customer using and how is access to those products being provided?
- Are those products more attractive or unattractive from a money laundering perspective (e.g. do they provide anonymity, such as with cash)?
- Do the products allow immediate access to funds?
- Do they allow for instantaneous international transfer of funds (e.g. SWIFT and telegraphic transfers)?
- Do they allow deposits to be made by third parties?
- Does the product facilitate the disguise of customer identity and - transaction ownership (e.g. special use accounts, omnibus accounts, bearer instruments, beneficiaries, etc.)?

- Is the product distributed directly to the customer by the financial institution's branches, or via a network of independent salespeople/intermediaries?
- Does the product attract customers without face-to-face interaction (e.g. via the internet)?
- Does the product provide enhanced levels of discretion and security (e.g. private banking)?

Transaction types

- Are transactions on the accounts typically in very high amounts?
- Is there an especially high transactional volume?
- Are they 'payable through' transactions (i.e. where the account is neither the originator nor the ultimate beneficiary)?
- Are the economic reasons for the transactions clear and justifiable (e.g. bill payment, purchase of goods, etc.)?

All the above indicators will affect a particular relationship's susceptibility to money laundering and terrorist financing. Each organisation should, through its policies and procedures, set out clearly through a risk assessment methodology how each risk factor is measured (e.g. applying the Basel AML index for country risk) and what weight will be given to each factor thus determining what level of risk a potential customer is.
Under the risk-based approach, what financial institutions then need to do after risk analysing their customer relationships, is to design and implement management and operational controls that are appropriate for and commensurate with the level of risk identified.

MITIGATING CONTROLS

In management and operational terms there are various aspects of policy and control that can be adjusted according to perceived risk levels, with more stringent, enhanced controls being applied to higher-risk relationships

and less stringent, simplified controls being applied to lower-risk categories.

Identification requirements

For lower-risk relationships, a single form of identification and address verification may be appropriate. For higher-risk relationships, a greater degree of background research (and corresponding supporting documentation) as to identity, history, residence and other aspects of a customer's identity may be deemed necessary.

Management approvals required for customer acceptance

If a customer is categorised as low risk, there ought not to be any need for senior management approval before they are accepted as customers. For higher-risk customers, however, the approval of more senior management may be appropriate and necessary and for the highest-risk customers, it may even be appropriate for the board of directors to sign off on the relationship.

Due diligence and KYC information

If a customer is in a lower-risk category, there may be very little point in making extensive enquiries about their background, the nature of their income and their activities and operations (indeed in many cases this will be obvious, e.g. a salaried individual). For higher-risk customer groups, however, these types of enquiries make a great deal of sense because they increase the financial institution's understanding of the customer and hence its capability to detect unusual and potentially suspicious behaviour. Enquiries might relate to, for example, further information on the nature of the business relationship, source of funds, sources of wealth (where appropriate), the reasons for intended and performed transactions, etc.

Frequency and depth of account monitoring activity

For lower-risk customers it may be appropriate to do a limited amount of transaction surveillance focusing only on detection scenarios appropriate to the type of customer (e.g. simple financial thresholds for individuals). For

higher-risk categories, more frequent and extended transaction surveillance would be appropriate (e.g. using detection scenarios that consider the percentage variance in deposits and debits over a given period, and single 'one-off' transactions). Additionally, sample sizes can be increased and transaction thresholds reduced to provide closer monitoring. In the highest-risk cases it is possible to conceive of 24/7 monitoring, but at those extreme risk levels one would have to query whether a relationship should exist at all. In most cases these exceptions will be 'post' event (i.e. after the transaction has taken place) but again, in the highest risk cases it may be appropriate to consider 'blocking' a transaction particularly in countries where there may be a requirement for consent to be given where suspicion is raised.

Assurance and audit/independent testing

The level of assurance and audit of the three-line defence model described in Chapter 3, should be adjusted according to risk. For example, higher-risk businesses should have more regular and detailed assurance testing and be audited with greater frequency and to a greater width and depth of sampling than lower-risk businesses.

Communication, training and awareness

Within the overall control environment, it would be appropriate to focus greater resources on training and awareness within higher-risk business units at the justified expense of those businesses deemed to be lower risk, provided that all statutorily required basic training requirements for the organisation have been covered. There should also be detailed training for those relevant staff involved in higher-risk business areas or customers (e.g. correspondent banking, PEPs (Private Banking)).

REGULATORY ENVIRONMENT

The risk-based approach effectively represents a trade-off between regulated firms and regulators. In return for a more business-focused, less bureaucratic form of regulation, financial institutions have accepted a greater burden to analyse risks effectively and act accordingly. The implication is that if they fail to do this then the censure and punishment they face will be even greater than before.

Table 4.1 shows an example of what one particular financial institution considered to be high-risk characteristics from an AML perspective. Read the categories and then take a moment to consider how appropriate it is for your own organisation. Consider whether there are any items that you would add or delete from any of the columns with regard to your own business.

Table 4.1 **High-risk characteristics**

Customer/ business types	Geography	Product/delivery channel	Transaction types
Politically Exposed Persons Non-residents Money service businesses and virtual currency exchanges Gaming and betting Real estate brokers Jewellery businesses Car, boat and aircraft equipment dealerships Charitable organisations and NPOs Law and accounting firms Pawnbrokers Phone or debit card companies Offshore trusts	Sanctioned countries High-risk countries (e.g. 311 USA Patriot Act and FATF)	Private banking Trusts Retail involving high net worth individuals and their corporate interests with high levels of personal service Internet delivery Nominee accounts Prepaid stored valued cards	Offshore Foreign wire transfers, money instruments and cash 'Omnibus' and 'concentration accounts' E-bill payment services Correspondent bank clearing Payable through accounts

SPECIAL CATEGORIES: POLITICALLY EXPOSED PERSONS (PEPS)

A category of high-risk customer that receives particular attention in the various international standards and guidelines (FATF 40, BIS, Wolfsberg, EU Directives, USA Patriot Act) is that of Politically Exposed Persons (PEPs). PEPs are defined in the FATF 40 recommendations (interpretative notes section) as follows:

> **'Foreign PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.**
>
> **Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, i.e. directors, deputy directors and members of the board or equivalent functions.**
>
> **The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.'**

Source: www.fatf-gafi.org copyright © FATF/OECD. All rights reserved.

Why are such figures considered higher risk from an AML perspective? The reasons stem mostly from the high profile that such individuals hold. They tend to attract a great deal of interest from business people, some of whom may have criminal connections or may even be criminals themselves. They often have substantial decision-making powers (or, in democratic states, the prospect of obtaining these powers through the political process) including the power to allocate vast state funds to particular companies through the award of government contracts. This therefore makes them vulnerable to bribery and corruption. In the worst instances, they may even themselves be of a criminal disposition whereupon they will be well placed to misappropriate public funds. Finally, of course, by virtue of their positions they are likely to be in possession of sensitive non-public information

which could enable them to benefit in a criminal manner at the expense of others (e.g. insider trading), should they choose to use it that way. And because PEPs are aware of the scrutiny which their activities are likely to be subject to, they may use family members, associates and completely unknown 'fronts' as conduits through which to conduct their transactions and escape scrutiny.

Recommendation 12 requires that financial institutions should, in relation to both foreign and domestic PEPs, and in addition to performing normal due diligence measures, have appropriate risk management systems to determine whether the customer is a PEP. Once such a determination has been made, then in relation to all foreign PEPs and in relation to domestic PEPs whom they have assessed as being higher risk, financial institutions should:

- obtain senior management approval for establishing business relationships with such customers
- take reasonable measures to establish the source of wealth and source of funds, and
- conduct enhanced ongoing monitoring of the business relationship.

Clearly, the capability of an organisation to determine whether a prospective customer is a PEP is an important one. But how do you determine whether an account holder is a PEP? There are various methods available:

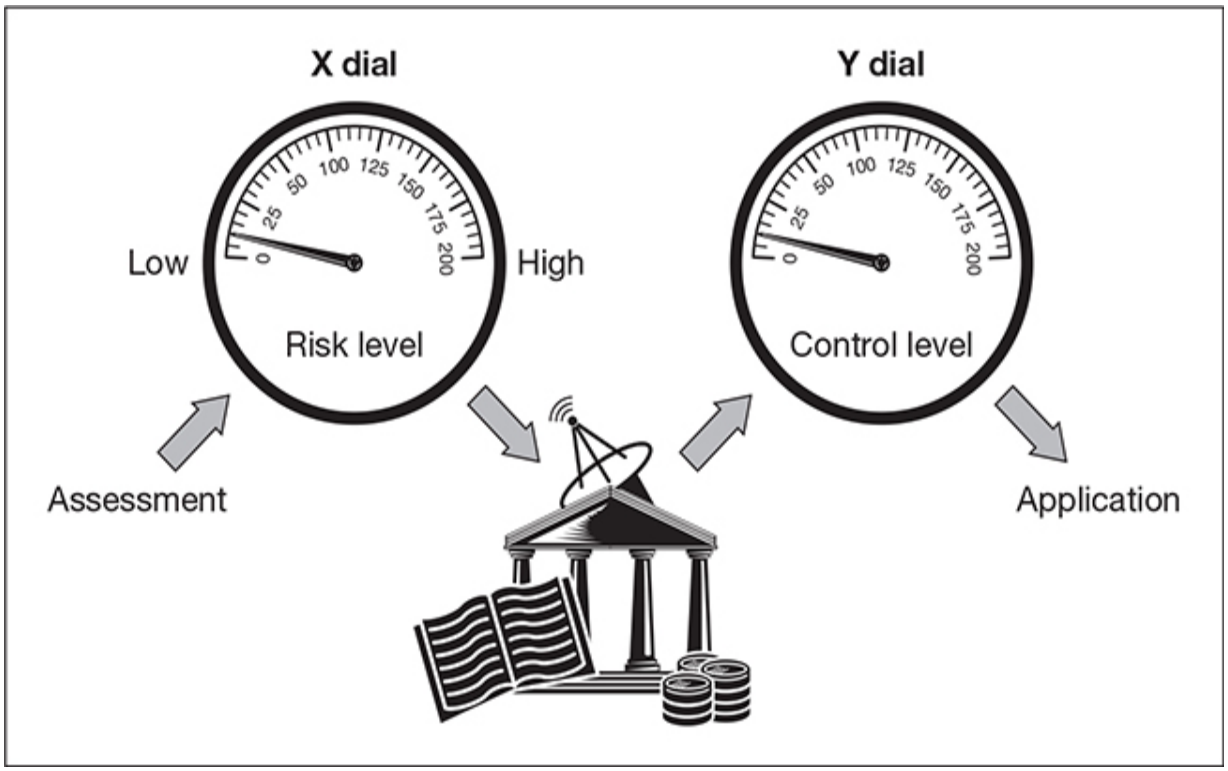
- seek information directly from the individual
- review sources of income including past and present employment history and references from professional associates
- review public sources of information (e.g. databases, newspapers, microfiche records, etc.)
- check the Central Intelligence Agency (CIA) online directory of 'Chiefs of State and Cabinet Members of Foreign Governments' (www.odci.gov/cia/publications/chiefs/index.html)
- check the Transparency International Corruption Perceptions Index
- check private vendor sources (e.g. Factiva, Thomson Reuters and Mimiro).

CONSTRUCTING A RISK-BASED APPROACH FOR YOUR ORGANISATION

Basic model examples

The risk-based approach (as described above) is already a regulatory requirement in many jurisdictions and will progressively spread to all jurisdictions, as they move towards full compliance with international AML and CFT standards. Care needs to be taken that risk-based solutions which are in keeping with international standards are nevertheless still consonant with national regulatory requirements.

Figure 4.3 **Risk-based approach assessment and control model**



Conceptually, it is helpful to think of the process of designing risk-based controls in terms of having two dials, X and Y. The X dial is connected to antennae capable of gathering relevant information and it records risk according to the various criteria discussed above. The Y dial is adjustable and sets control levels. It can be calibrated, according to the risk information received from the X dial, so as to provide the optimum control environment for the institution. This model is depicted in Figure 4.3.

In terms of risk assessment, clearly organisations must be able to harness as much high-quality information as possible in order to make a meaningful assessment of risk. Questionnaires, therefore, for completion by the customers themselves or by bank staff, paper-based or electronic, will be an important medium through which information about the customer is acquired. Other important data-gathering media include well-structured interviews, background research (where this is justified) and, in extreme cases, private vetting via investigations agencies (more on this in Chapter 5, which deals with the subject of reputational risk).

Information about the customer needs to be married with an assessment of the product risk and country risk, as discussed above.

Product risk assessment – test your instincts

What makes a product more or less risky from an AML and CFT perspective? We looked at some of the features earlier on and now we will try to put these into practice. Below are some product descriptions from different areas of financial services. Look at these descriptions and for each product assess whether you consider that product to be either higher or lower risk.

Banking

Product: Personal Current Account – *High or Low Risk?*

Product: Personal current account

Description: Ordinary account for daily living

Surrender/withdrawals: Yes

Payment methods: Cash, cheque, draft or transfer

Third-party payments: Yes

Additional payments: Yes

Minimum periods: None

Complex structures: Possible

International: Possible

Other controls: Identification requirements on account opening

This product may be high risk for placement and layering activity, but will only normally be considered high risk if the amounts going through it are large. It satisfies many of the launderer's requirements. It can receive money, in cash if needs be, and from third parties, and send it anywhere in the world to other third parties. There are no limits to the amounts which can be put through it (subject to staff suspicions) and no minimum periods or lock-ins. As such, the management of the risk should be focussed on the risk of the customer, the due diligence to be applied and effective transaction surveillance.

Product: Letter of Credit/Documentary Credit – *High or Low Risk?*

Product: Letter of credit/documentary credit

Description: Trade finance product through which bank pays exporter for goods and reclaims funds from importer

Surrender/withdrawals: Yes, value is exchanged at the point where bank accepts reimbursement from importer

Payment methods: Cheque, draft or transfer

Third-party payments: Yes

Additional payments: No, but multiple credits possible for single clients

Minimum periods: None

Complex structures: No

International: Yes

Other controls: Fraud controls on import/export documents

These products are medium to higher risk within the banking sector. Letters of credit can be and are used for money laundering (typically layering), despite being vulnerable to discovery from vigilant trade clerks who may, for example, recognise that the import documents are fake.
The determination and management of the actual risk depends on who the actual customer is and who their trading counterparts are. This could require intrusive scrutiny (e.g. credit checks, adverse media checks) of the customer to discover whether it is a proper trading company, or through a registered office visit to verify that the business is as it claims to be. This could also include some limited due diligence in those counterparts.

Product: Credit Card – *High or Low Risk?*

Product: Credit card

Description: Running credit account based on point-of-sale credit transactions, with balances and/or interest repaid monthly

Surrender/withdrawals: Yes, value is exchanged at the points where (1) goods and services are purchased, and (2) debit balances incurred are repaid

Payment methods: Cash, cheque, draft or transfer, but amounts are usually small, less than €5,000.

Third-party payments: Yes, but would be considered unusual

Additional payments: Yes, payments are made monthly

Minimum periods: None

Complex structures: No

International: Yes

Other controls: High predictability of profile on most accounts allows easy identification of unusual card usage

Credit cards are lower risk because they are not as flexible as, say, a current account (you can do fewer things with them.) But they can be used by criminals at the integration stage – particularly at the platinum end of the -market – for unlimited spending, with funds of criminal origin used to repay the card. Credit card frauds can also be used to finance terrorist attacks.

Product: Corporate Treasury Foreign Exchange Services – *High or Low Risk*?

Product: Corporate treasury foreign exchange services

Description: Conversion and transfer of currency deposits, both for trade/commercial purposes and as part of speculative/trading strategy. Often large sums involved (more than €1 million)

Surrender/withdrawals: Yes

Payment methods: Cash (rare, given amounts), cheque, draft or transfer

Third-party payments: Yes

Additional payments: Yes

Minimum periods: None

Complex structures: Often

International: Yes

Other controls: Services often offered only to limited pool of well-known institutions

These products are higher risk, given the large sums involved and the international nature of the business, allowing substantial cross-border payments to be made to and from an account. The risks can be mitigated by limiting availability, as above.

Fund management

Product: Hedge Funds – *High or Low Risk*?

Product: Hedge funds

Description: Non-discretionary investment for sophisticated investors with high-risk appetite (e.g. may involve derivatives trading and short selling)

Surrender/withdrawals: Yes, but usually a lock-in for a set period (e.g. five years)

Payment methods: Bank draft or electronic transfer

Third-party payments: Yes

Additional payments: Yes

Minimum periods: Five years and beyond

Complex structures: Yes

International: Yes

Other controls: No

These products are higher risk due to the fact that they allow a diverse range of investors, as well as the use of complex investment structures and some offshore tax havens with a lower degree of regulatory scrutiny.

General insurance

Product: Personal Household Insurance – *High or Low Risk*?

Product: Personal household insurance

Description: Household insurance for contents and buildings

Surrender/withdrawals: Upon a claim

Payment methods: Monthly or annually

Third-party payments: By the broker

Additional payments: For increases in contents liability

Minimum periods: Annually

Complex structures: No

International: Possibly, subject to permissions in the overseas country

Other controls: Fraud claims. If payment stops so does policy.

This would be low risk, due to the fact that payout only occurs after assessment. Also a police crime reference number has to be provided. If premiums cease so does the cover. Fraud controls will also be in place.

Adjusting product controls to the overall level of the relationship risk

As we have seen, AML and CFT risk is about more than just the product. It also encompasses the type of customer, geographic issues and business issues. As mentioned above in order to make the risk-based approach work, organisations need to construct methodologies for applying particular control regimes to a particular type of risk – assessed relationships. At a basic level, one can imagine a process as follows:

- consider product, distribution channel, customer and domicile
- consider whether high-risk elements shift the relationship into a higher-risk category (e.g. a high-risk customer using lower-risk products)
- adopt increasing control strengths according to whether a relationship has been assessed as either 'low', 'medium' or 'high'. For example:

  Low risk = A + B (i.e. minimum legal requirement of customer identification (A) and address verification (B))

  Medium risk = A + B + C (i.e. identification plus address verification plus source of funds check (C), i.e. where the funds have originated from – e.g. bank, private account)

  High risk = A + B + C + D (i.e. identification, address verification and source of funds check as above, plus source of wealth check (D), i.e. what economic activity has generated the customer's wealth?)

Transaction surveillance activities are also adjusted accordingly, such that very limited surveillance takes place on low-risk accounts, increased surveillance taking place on medium-risk accounts and a very frequent in-depth surveillance occurs on high-risk accounts.

It is important to note that a low-risk product could be placed in a higher-risk category if the customer is perceived as a high risk (e.g. a politically exposed person using a credit card).

It is worth considering how an organisation manages the fact that a customer's risk level could change through the life-cycle of the relationship. This could be because they change their business type from low to high risk, or they change their countries of business from low to high risk or change from being non-resident to resident (high to lower risk).

This is normally managed through what are known as Periodic Reviews. These are regular reviews of a relationship at given set time periods based on the risk level which was determined at onboarding. A common practice would be at one-year intervals for high-risk customers, two years for medium and three years for low-risk customers.

In addition, most organisations will perform such reviews at 'trigger events' when they become aware of such changes through customer interaction.

These reviews should consider the CDD and KYC information held and determine if there are any significant factors (as exampled above) that would change the current risk rating.

These reviews should also look at the transactional behaviour of the customer since the last review to ascertain whether it is consistent with the due diligence/KYC on file.

This approach is still common practice and valuable in a pure relationship managed segment such as, for example, medium to large corporations. However, in a 'mass market' such as individuals this can be a burdensome approach given the sheer numbers and the processes required to ensure they are completed at the appropriate points and in a timely manner. Trigger event reviews are particularly difficult to manage in this regard and regulators tend to look carefully at the periodic review process to ensure it is managed effectively and with few 'overdue reviews' being reported.

In light of this, some organisations now look to manage this 'dynamically' by using their core banking and transaction surveillance systems to automatically 'alert' them when there are changes to the customer profile

and thence manage the review through to closure with a case management system.
In simple terms there are two types of changes to the customer profile held that could affect the risk rating, as well as requiring a review to be performed:

- static data changes (address, for example)
- behavioural changes (transactions, business operations).

A financial institution's core banking systems ought to be able to recognise such changes and, as mentioned, be capable of registering them as a 'trigger event' requiring a review. For those customers for whom there are no profile changes during the life cycle, the set periodic review date can be entered and the review and case management triggered at that time.
So, for example, a customer might write in to advise that they have changed their address from the UK to Nigeria, thus becoming non-resident. Based on this information, the core banking system would automatically amend the risk rating from Low to High and create a trigger event for a review as there could be a requirement for more detailed due diligence to be performed, as per the CDD requirements for higher-risk clients.
Another example could be that, while not suspicious and thus requiring a STR, the transactional behaviour of the customer has generated an 'unusual activity' alert on the transaction surveillance system, which then presents an opportunity to engage with the customer to find out more and – if warranted – to then review and raise the risk rating for higher level CDD and possibly file a STR as well.
The benefits of this dynamic risk rating and periodic review process are that it is automated and recorded, with a clear work flow that is transparent to regulators. It also enables organisations to reduce the error rates which tend to be endemic with a manual approach.
This approach should be supplemented with regular encouragement to customers to advise of any changes to their circumstances, so that their CDD information is kept up to date. This encouragement can be with messages at ATMs, messages through on-line banking and, where paper based, messages imprinted on their bank statements, for example.

Relationship risk classification – test your instincts …

Using the above methodology, we can now review some relationship examples and try to ascribe a risk assessment rating (low, medium or high) and a corresponding control regime (A + B; A + B + C; or A + B + C + D) to each example. Note that at this stage we are not using a consistently applied calculating mechanism (that comes later). Rather, we are exploring how different combinations of customer, product and geographic risk factors affect our assessment of risk and the different control responses required accordingly.

Scenarios

Scenario 1

An individual customer from a FATF member country wants a credit card, which will be repayable from their current account at an EU regulated financial institution. The predicted average monthly spend on the card will be around €800.

This scenario involves a low-risk product, a low-risk customer, a low-risk jurisdiction, with low regular payments from a regulated financial institution in a low-risk low-risk jurisdiction = a low-risk relationship. So A + B would be appropriate – identity check and address verification, with the least intensive monitoring.

Scenario 2

A government official from a highly corrupt country wishes to open a numbered deposit account with your private bank, with the initial funds being transferred from the accounts of nominee companies owned by him in various offshore locations, some of which have been associated with tax evasion. The initial expected receipt is for USD 2 million.

This scenario involves a high-risk product, a high-risk customer, a high-risk jurisdiction, a very large initial deposit (given the applicant's

occupation) = a high-risk relationship. In fact, even allowing for A + B + C + D (identification, verification, source of funds and source of wealth checks) – query whether you should be doing this business at all unless you can get some compelling evidence on the legitimacy of the applicant's source of wealth.

Scenario 3

A trading company wishes to open letters of credit for products being exported from a FATF country to a neutral country (i.e. neither FATF nor ICRG). Payments under the credits are to be received from the importer's local bank. The products in question are perfume and certain other fancy goods.

This scenario involves a medium–high-risk product, a low-risk customer, and a medium-risk counterparty (the paying bank) from a medium-risk jurisdiction = a medium-risk relationship. So A + B + C would be appropriate – identity check, address verification and source of funds check. You would also need to conduct due diligence against the importer's bank. In the highest risk scenarios for trade-related products, consideration needs to be given to any due diligence on the non-customer third parties (importer/exporter) to the transaction.

Scenario 4

An established institution from a FATF country wishes to make a medium-sized investment in one of your property funds (an investment fund containing a portfolio of commercial property and producing income from rental streams and profits on sales from properties located in the EU, the US and Hong Kong; investment range from USD 10m to 25m)

This scenario involves a relatively low-risk product, a low-risk customer, low-risk jurisdictions and a moderate investment sum = a low-risk relationship. A + B only are appropriate – identity check and address verification, with minimal monitoring

Scenario 5

A previously unknown firm of investment consultants from an offshore tax haven states that it represents a group of international private investors with a high-risk appetite and a very large amount of money for investment in your best performing hedge fund.

This scenario involves a high-risk product, a high-risk customer, a high-risk jurisdiction and large investment amounts = a high-risk relationship. A + B + C + D is required – identity check, address verification, source of funds check and source of wealth check.

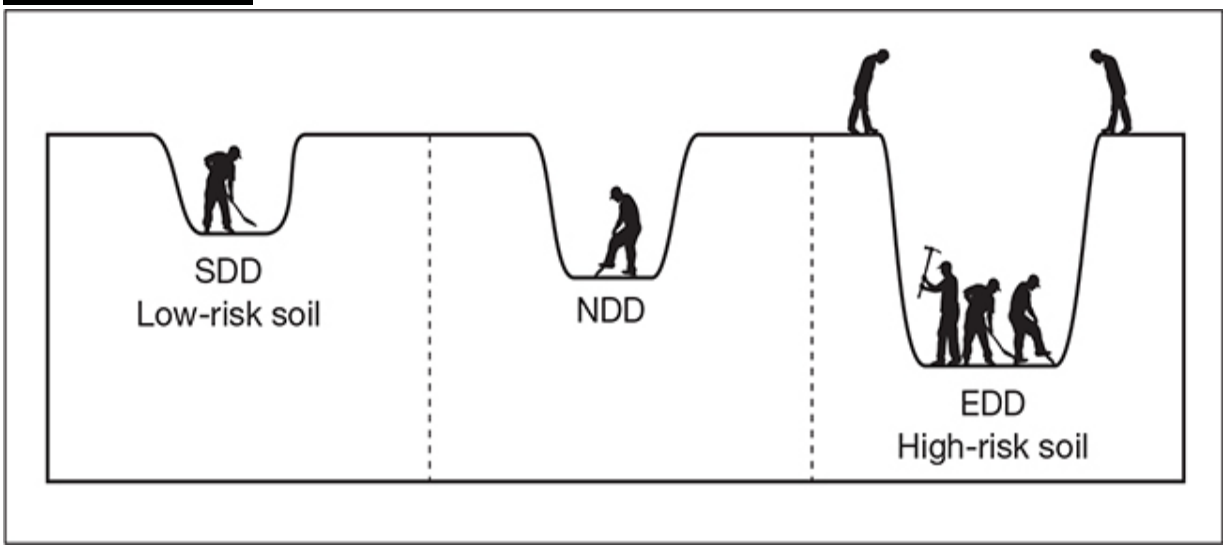
Taking it to the next level of detail

Building upon the principles outlined in this chapter, you should think of due diligence as a process of digging for information (see Figure 4.4) . If a relationship is very straightforward and low risk, then you're not expected to dig very deep and a simplified form of due diligence (denoted as Simplified Due Diligence – SDD Figure 4.4) will be appropriate, involving only a restricted number of the information elements listed above. Depending on the business profile of your institution, this may actually be a relatively small minority of the overall number of customer relationships. There will then be those customers and relationships where the risks are of a medium nature with much more digging required in many more of the key information elements listed above (designated as Normal Due Diligence – NDD). Again, depending on the specifics of the institution's business profile, this category may turn out to encompass a significant majority of its overall customers and relationships.

Finally, there will be those relationships which are classified as high risk, for the various reasons that we identified earlier on in this chapter. These

will require the greatest depth of digging. The purpose of this digging is not just to increase the chances of identifying information and previously unknown risks that may affect your decision to take the customer on or affect your treatment of them, if you are already in a relationship with them. The digging also ensures that you can demonstrate to the world at large that you took greater precautions when you perceived higher degrees of risk. For these high-risk relationships the full range of information types outlined above would need to be collected. This level of quite intensive 'digging' is designated as Enhanced Due Diligence (EDD in Figure 4.4) .

Figure 4.4 **Digging deeper for information**



THE CORE COMPONENTS OF CDD

Information collection

Whatever risk assessment framework you are operating, the due diligence which your company undertakes will comprise the base level elements of information collection and information verification.

The type of information which it may be relevant to collect for due diligence purposes is wide ranging. Details could be required, for example, in relation to any or all of the following.

Personal information

- name – including any aliases, shortened versions and variations in the order of the words in the name (e.g. 'John Vey Atta', also known as 'Atta John' or 'Vey John')
- address – including alternative addresses where these exist
- date of birth
- nationality
- occupation
- source of funds – i.e. the location (country/city) and bank or other institution from which funds entering the account have originated and will be on-going
- account purpose – the reason why the account is being opened (e.g. to receive salary; to purchase a new car; to set aside funds for investment, etc.). This is a critical piece of information which, all too often, is completed by relationship managers in insufficient detail. Answers which the author has seen on customer acceptance documentation have included 'general', 'N/A' and even 'bank account'
- anticipated account activity – i.e. the types, size, volume or frequency of transactions anticipated to take place on the account
- source of wealth – the economic activity which has generated the funds or other assets which the institution is handling for the client (e.g. inherited wealth, wealth from the sale of a business, investment income, etc.).

Personal information of a corporate nature

It is not just for personal accounts that you may need to obtain personal information. Individuals obviously hold or perform key positions and functions in corporations and other legal entities, in which case the following information may be required:

- names and identities of directors and partners
- names of registered and beneficial owners holding (25 per cent or more significant percentage of the shares or voting rights in an entity.

This percentage is generally set at 25 percent but many organisations are now applying 10 per cent in higher-risk scenarios). ('Beneficial owners' may not appear on share registers, and are natural persons – not corporate entities – who ultimately own or control the entity, or for whose benefit or on whose behalf transactions are conducted)

- names of all authorised signatories
- names of settlers, trustees and beneficiaries.

Corporate (non-personal)

Finally, there is information about the customer entity itself when it is an artificial person, such as:

- name
- registered number/tax identification number
- type of entity – e.g. private corporation, public/state-owned entity, partnership, etc.
- registered office
- business address (if different)
- country of incorporation
- purpose of account
- anticipated account activity
- the nature of the business – i.e. the business sector in which the entity is involved and any specialist products or services it provides
- countries where the entity conducts business – this would include, for example, export destinations and import origination, as well as details of overseas offices and branches, with special reference to high-risk countries and countries which are a subject of sanctions
- in case of financial institutions, information on internal AML and CFT policies and controls (see below on Wolfsberg questionnaires)
- details of reputation in terms of corporate activity
- quality of supervision
- reason for opening account
- source of wealth.

All of the above adds up to quite a lot of information and would impose significant burdens on most institutions if all of that information had to be

collected in each and every case. Thankfully, because of the application of risk-based principles, this isn't necessary.

Verification

What do we mean by 'verification'? Verification refers to the process by which we provide proof or reassurance that a piece of information is true.
If your institution has account opening discussions with a representative of a company who tells you that the name of the company is Bertoli Communications Ltd, how do you prove it? Because, remember, if you didn't prove it and the company was actually a different company or, more likely, non-existent, then money could be laundered through its accounts, those accounts could be emptied, everybody would disappear and there would be nothing left to go on.
If the representative of the company tells you that its business is the import and export of mobile phones and other electronic communications equipment, how do you prove it? If you don't, then it's possible that it could be a shell company and that all the activity on its account represents money laundering.
If the representative tells you that the beneficial owners of the company are Mr X and Mrs Y, how do you prove it? Because if you don't, how can you say that the company isn't owned by an organised crime syndicate or a corrupt politician?
Verification doesn't stop accounts and relationships being used for money laundering, but it is an important barrier, an inconvenient additional hurdle which criminals and launderers must overcome if they are to achieve their objectives. Verification involves the collection and retention of evidence in the form of official documentation (e.g. passports, constituent documents of companies and other artificial legal persons, print-outs from websites), certification (e.g. certifying copies as being true copies of originals which have been sighted, and stamping documents as such, obtaining official letters from embassies, notaries, solicitors or attorneys regarding the truth and reliability of documents and copies of documents), reportage (e.g. a report prepared by a relationship manager of a visit to an address, confirming that the company is actually operating a business from that address) and electronic data (with the emergence of the data-driven economy over the past 20 or so years, increasingly now in a growing

number of countries there are reliable, independent databases which can serve as a means of electronic verification of, for example, addresses and telephone numbers against names and dates of birth).

The extent of information verification will, like the collection of the information itself, be undertaken on a risk-sensitive basis. The higher the perceived level of risk, the more extensive the degree of verification that is required. As we shall see, in the highest-risk relationships involving, say, politically exposed persons or companies operating in very high-risk sectors or countries, the required information and verification levels may be quite extensive and will involve asking lots of questions and checking the answers against a wide range of documents such as trade agreements, financial returns, solicitors' letters, press articles, business sale agreements and property deeds. There are also multiple sources of publicly available information which can be used to check the consistency of information which has been provided to you, though it should be remembered that the easier it is for the information provider to manipulate such sources, the less reliable they are. Examples include:

- company website and literature
- Google and other search engines
- newspapers and other media (including their websites)
- industry magazines and websites
- local and industry contacts and other third parties
- subscription information services such as Factiva and Thomson Reuters.

In certain situations (which we explore in more detail in Chapter 5), it may prove necessary to instruct external agencies and consultants to conduct investigations against individuals and companies in order to establish their bona fides.

Long gone are the days when it was acceptable to 'take a gentleman at his word', as the bankers in Victorian Britain used to put it.

CDD PROCESSES AND TOOLS

In the wholesale/corporate, financial institutions, retail/consumer and wealth management/private banking example processes which follow, I have suggested a common framework and some common tools with which to inform a tactical approach to implementing the broad principles of the risk-based approach. This framework is shown in Figure 4.5.

Figure 4.5 **Example CDD process**

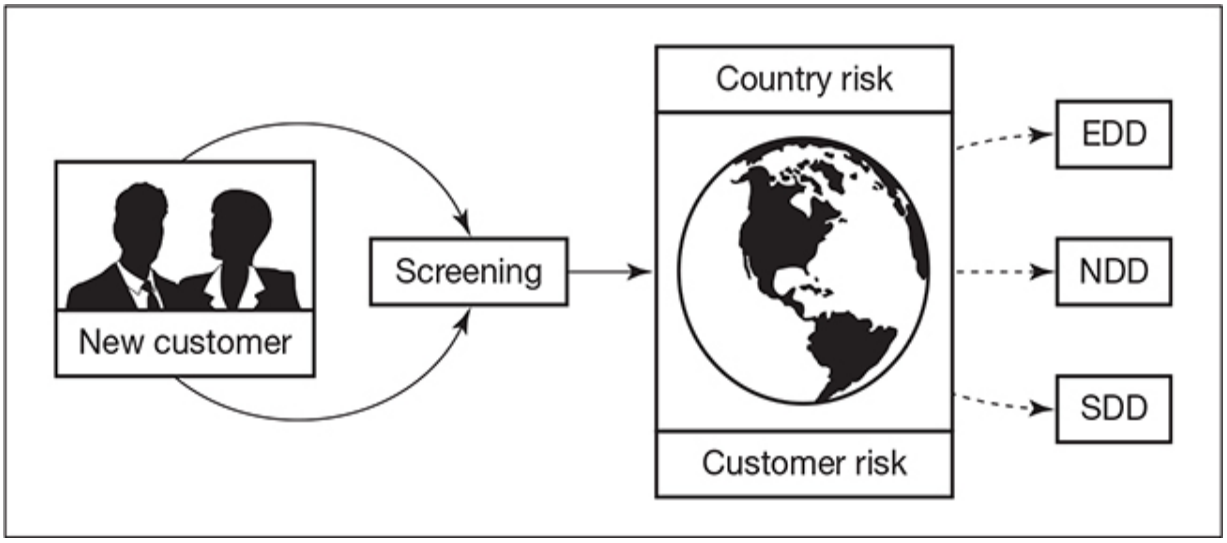


Figure 4.5 echoes the earlier generic client acceptance process flow described in Chapter 3. At various stages, systems, procedures and controls must be in place to enable your institution to:

- screen applicants for business against a company watch-list of prohibited entities and prohibited account or relationship types
- reach meaningful assessments of country, customer and product risk, based on a clear risk assessment methodology
- classify relationships into one of three categories which I have designated as simplified due diligence (SDD), normal due diligence (NDD) and enhanced due diligence (EDD)
- calibrate information, verification, approval levels, account monitoring and audit intensity according to the level of perceived risk
- review relationship activity on an ongoing basis (again, risk-sensitive) and recalibrate where necessary.

Unacceptable clients and relationships tool

Apart from your institution's alert-list requirements, a key tool during the screening stage of the process will be your list of unacceptable accounts and relationships. This will be based upon both generally accepted practice and your company's own risk appetite based upon its own experience (things which have gone badly, gone well or could go well if they were managed differently, etc.).
Here is an example of one such list:

Example

Institutional list of unacceptable accounts/relationships

- Proscribed entities
- Shell banks
- Unlicensed banks
- Unregulated money service or crypto exchange businesses
- Customers with known or suspected involvement in money - laundering, terrorist financing, WMD proliferation or tax evasion
- Anonymous or numbered accounts

In other words, this is your institution saying to the world: 'We are not even going to go to the trouble of assessing risk here, we simply will not do this business – ever.'

Country risk list tools

Clearly you cannot rely on individuals or business units to make their own assessments of money laundering and terrorist financing risks in different countries on an ad hoc basis. They will need a list, updated regularly, which designates every country in the world as either low risk, medium risk or high risk for money laundering, terrorist financing and, latterly, for

international tax compliance and proliferation financing. There are companies and commercial websites selling consultancy services and collated publicly available information that can assist you in determining which category a country should fall into. This is also something which you and your institution should spend some time thinking about. Relevant factors include:

- economic sanctions
- presence on the FATF ICRG list
- offshore status (and if so, current status on the OECD managed tax information exchange agreement process)
- any Moneyval, WorldBank or IMF mutual evaluations or assessments of the strength or otherwise of the country's AML regulatory regime
- membership of bodies such as the FATF or its regional sub-groups
- membership of the EU
- political unrest, war, insurgency or terrorist threat
- whether a producer or transit country, for example, narcotics, people trafficking or smuggled goods such as weapons, alcohol and tobacco
- any specific features of its financial services industry which make it higher risk (e.g. tax advisory, nominee/trust companies, private banking)
- any institution specific incidents or beliefs relating to that country (e.g. based on knowledge of local business practices).

Country risk lists, particularly those from governmental or regional - institutions, are obviously useful in assessing the comparative risks of different jurisdictions. However, the fact that a country is listed on a 'low-risk country' list is no guarantee that all business within that country is automatically low risk. In the same way, it's important to remember that just because a country is an EU member state doesn't automatically mean that it should be treated as 'low risk'. For example, for different reasons, a number of financial institutions rate e.g. Estonia, Luxembourg and Greece as 'high risk', even though they are EU member states. Likewise, most financial institutions rate Russia as 'high risk' even though it is a member country of the FATF. People form their own judgements and so should you and your institution.

Table 4.2 shows a sample example of a country risk-assessment sheet, - followed by a list of equivalent jurisdictions in Table 4.3.

Business sector risk tool

Again, your business units will need policy guidance on this, as individual perceptions of risk will differ. What makes a business high or low risk for money laundering and terrorist financing purposes? To answer that question one must look at how attractive certain business types are for those who wish to launder money or finance terrorism. Clearly cash-based businesses are attractive for the reasons we have identified earlier, as are any businesses involved in the transmission of money for other people. Import and export companies with a valid business reason for remitting and receiving large sums in their normal course of business will also be high risk for their 'cover' potential for money launderers, and we know that the real estate sector also offers attractive opportunities for money laundering. Religious organisations, charities and non-profit organisations (NPOs) are high risk for terrorist financing.

In terms of medium risk, these would be business types which have some potential for money laundering and which, while not offering the same level of attraction as the high-risk business sectors above, nevertheless are known to have been involved in money laundering schemes, such as the construction industry, certain categories of business consultancy and professional services (lawyers, tax accountants, company formation agents, etc.) and the sale of computer equipment, mobile phones and technology.

Table 4.2 **An example country risk tool**

High risk	Medium risk	Low risk
Afghanistan	Angola	Armenia
Albania	Aruba	Australia
Belarus	Bahrain	Belgium
Burma	Cambodia	Botswana

Haiti	Cayman Islands	Brunei
India	China	Canada
Indonesia	Hong Kong	Chile
Iran	Hungary	Czech Republic
Iraq	Ireland	Finland
Liechtenstein	Jersey	France
Luxembourg	Kazakhstan	Germany
Macau	Malaysia	Ghana
Nauru	Malta	Greece
Nigeria	Mauritius	Iceland
Pakistan	Philippines	Israel
Paraguay	Singapore	Italy
Republic of Bissan*	Togo	Japan
Russia	Turks & Caicos Islands	Lithuania
Sao Tome and Principe		New Zealand
Switzerland		South Africa
Ukraine		

*used in examples later (not a real country)

Table 4.3 **An example jurisdictions tool**

EU member states		
Austria	Belgium	Bulgaria
Croatia	Cyprus	Czech Republic
Denmark	Estonia	Finland
France	Germany	Greece

Hungary	Ireland	Italy
Latvia	Lithuania	Luxembourg
Malta	Netherlands	Poland
Portugal	Romania	Slovakia
Slovenia	Spain	Sweden
Non-EU EEA member countries		
Iceland Switzerland	Liechtenstein	Norway
Non-EU FATF member and observer countries*		
Argentina	Australia	Brazil
Canada	Hong Kong	Japan
Mexico	New Zealand	Singapore
South Africa	United States of America	
*Observers may not always be regarded as equivalent under JMLSG guidance.		

Lower-risk sectors would be those which are not immediately and obviously attractive, or known in the past to have been associated with money laundering activity. As with country risk, consultancies will sell advisory services on business sector risk assessment for AML/CFT purposes. There is also publicly available information on business sector risk. In terms of how you go about creating the business sector risk list, there is no point in re-inventing the wheel. The best place to start is with the business type lists which your institution already has in place for credit assessments and other forms of business risk and opportunity analysis. An example is shown in Table 4.4.

Source of wealth information checklist tool

There will be occasions when, typically as part of enhanced due diligence (EDD) enquiries, business unit staff will be required to seek information to prove a customer's source of wealth. Although at first sight this may seem to be a fairly straightforward task of asking and obtaining information from

the customer, experience suggests that, in practice, staff – particularly in sales and relationship functions – need to be pushed to do it properly. They often feel that they are putting the overall relationship (and the revenue which comes with it) at risk by asking questions which may be deemed by the customer to be too intrusive. This is particularly so when dealing with the types of wealthy and high-profile clients who are precisely the kind of people from whom such information should be obtained (lest it should turn out that the significant sums which have been entering and leaving their accounts on a regular basis have come from illegitimate rather than legitimate sources). For this reason, such reluctance by staff must be overcome and a good practical way in which to do this is to provide firm and detailed guidance on the questions which they should be asking, as well as more skills-based guidance and training on how to solicit relevant information during the course of normal social interaction. There is more on this in Chapter 5, which deals with reputational risk.

Table 4.4 **An example business type risk tool**

HIGH RISK (sample)	
Antique dealers	Precious metals dealers
Art dealers	Real estate development – commercial
Auction houses	Real estate development – industrial
Computer and computer software/	Real estate development – retail
peripheral stores	Real estate development – residential
Cryptocurrency exchanges	Real estate development – others
Foreign exchange brokers and dealers	Religious organisations
(money service bureau – MSBs)	Restaurants and bars
Gambling/gaming related services	Retail sale via stalls/markets
General importers and exporters	Retail wine/alcohol stores
Manufacturing of weapons and ammunition	Sale of used automobile and other motor vehicles (wholesale

Motor vehicle dealers (new and used) (retail) Other credit granting Other monetary intermediaries Other recreational activities	Wholesale wine/alcohol Wholesale and retail of gems and jewellery
MEDIUM RISK (sample)	
General/special trade construction of buildings and civil engineering works Construction – residential Construction – industrial buildings Construction – commercial buildings Construction – retail buildings Construction – others Business consultancy Highway, street, bridge and tunnel construction Water, sewers, gas, pipeline construction Construction of dams and water projects	Communication and power lines construction Construction of railways Other heavy construction Other building completion works Other building installation activities Retail sale of pharmaceutical and medical products Renting of construction or demolition equipment with operator Sale of motor vehicle parts and accessories (retail) Maintenance and repair of motor vehicles
LOW RISK (sample)	
Land reclamation works Grain farming Oil palm Oil seeds or oleaginous fruit Tobacco farming Rubber plantation Sugarcane farming Cotton farming	Cocoa plantation Coffee plantation Tea plantation Other fruits, nuts, beverage and spice crops necessary Livestock farming Other animal farming, production of animal products

Manufacture and/or distribution of industrial products	Agricultural and animal husbandry service activities
Vegetables, horticultural and nursery products	IT consulting

An example of a source of wealth checklist is shown in Table 4.5.

Table 4.5 An example source of wealth checklist

Source of wealth generated from business ownership
Nature of business and operations
Significant products and/or services?
Market penetration?
Geographic trade areas?
Number and identity of locations?
Number of people employed?
Details (percentage) of applicant's ownership of the business?
Ownership of the business
Names of other owners and their percentage ownership?
Estimated annual sales volume?
Estimated annual net income?
Length of time during which applicant has been involved with business?
Are there significant revenues from government contracts?
Business history
How long has the business been in operation?
How long has the applicant been in this particular business?
How was the business established?
Is the company publicly traded?

Source of wealth derived from a senior executive position
The individual What is the person's position in the company (e.g. managing director, chief executive officer, chief operating officer, etc.)? Length of time at the company? Area of expertise? Details of compensation (salary, bonus, share options, etc.)? (Note: look out for any differences between total stated and apparent net worth and compensation × number of years.) *The company* What is the business of the company? (Note: a good degree of detail should be provided. General answers such as 'financial services' or 'manufacturing' are insufficient. There should be a reasonably detailed description of what the company specialises in, unless it is a well-known global brand.)
Source of wealth derived from a profession (e.g. accountant, lawyer, doctor)
What is the profession? Are there any areas of specialism? Any previous employment history prior to joining the profession? Practice licence details? How is wealth derived from the profession? (For example, charge-out rate per hour/day × number of hours/days per year less estimated costs = net income, multiplied by number of years with appropriate reductions for lower earnings.) Strength of business reputation? (For example, prominent clients, details of academic/professional publications, advertisements, membership of professional bodies and position in local society – e.g. Round Table and other associations.)
Source of wealth derived from PEP status
Elected or appointed? Number of years in office or position? Any available public information (particularly negative information)? (Note: refer to Chapter 5 on reputational risk for a more detailed checklist on this issue.)

Main responsibilities (including responsibility for specific business sectors such as construction, transport, power, etc.)? Any known associations or interests in business entities?
Source of wealth derived from inheritance
From whom were the assets inherited? When were they inherited? What was the type and value of the assets inherited? How have the assets been dealt with since the time of inheritance (e.g. public and private investments, property, business venture)? (Note: you should be able to relate current wealth, by means of calculation, to any originally inherited wealth plus whatever has been earned from other sources such as employment or investment. Significant gaps between the amount originally inherited and current wealth need to be explained.)
Source of wealth derived from investments
List all assets by name, type (e.g. shares, bonds and other securities, fund and hedge fund investments, insurance policies, stakes in private businesses and franchises), value and growth in value since the investment was made. What was the original source of wealth for the investments (see above)? Any significant/high-profile transactions (e.g. private equity acquisition and disposal, involvement in hostile takeover, disposal of significant stake)? Estimated annual income from investments? Length of time client has been an investor?

CDD documentation tools

The requirement in the FATF standards is that financial institutions should undertake customer due diligence measures against their customers when establishing business relations and when carrying out occasional transactions which fall within certain parameters. This immediately raises a practical issue. There is a large array of different types of customers of varying legal compositions. It's possible that your company might have to conduct CDD against any of the following:

- individuals

- smaller companies in the private sector
- more well-established, substantial private sector companies
- publicly listed companies
- governments
- state-owned corporations
- regulated financial institutions and correspondent banks (dealt with in the next section)
- partnerships
- trusts and foundations
- non-government organisations
- charities
- clubs, societies and unincorporated associations
- entities conducting one-off transactions above certain financial thresholds
- if you are a large international group, introductions from other business units in other countries.

Your procedures will need to be very clear in terms of what information and documentation is required in relation to each in different circumstances, and the verification methods used. For these purposes you will require a detailed set of tools which show staff what types of documents must be obtained from customers and about different types of customers during the CDD process, for each of the different due diligence risk classification levels (SDD, NDD and EDD).

All such tools are not reproduced in detail here, but would basically comprise the legally required identification and verification documents for each of the above categories of customer.

The following example shows a CDD documentation tool for corporate customers, showing the different documentation requirements depending on whether the customer is classified as SDD, NDD or EDD.

Example

CDD documentary requirements for corporates

Simplified Due Diligence (SDD)

Identity and due diligence information:

- Company number
- Registered office in country of incorporation
- Business address
- Purpose and reason for opening the account or establishing the - relationship (unless obvious from the product)
- The expected type and level of activity to be undertaken in the relationship (e.g. total account turnover, largest expected balance (CR/DR)).

Verification:

1. Evidence of listing of publicly quoted companies (e.g. copy of relevant internet page published by the regulated market). Evidence of existence of government entity (e.g. copy of web page from government website).

2. The majority ownership status of any subsidiary.

3. The licensing and regulatory regime status of the company (e.g. letter from regulator confirming that the company is regulated).

4. Authority of authorised signatory(s) to open and operate the account (e.g. board resolution/mandate or government authorising document).

Normal Due Diligence (NDD)

Identity and due diligence information:

- Full name
- Company number or other unique identifying number assigned by government to the entity (e.g. taxpayer identification number)
- Registered office in country of incorporation
- Business address

- Purpose and reason for opening the account or establishing relationship (unless obvious from the product)
- The expected type and level of activity to be undertaken in the relationship (e.g. total account turnover, largest expected balance (CR/DR))
- Names of all directors, partners, proprietors
- Names of all beneficial owners
- Names of shareholders owning at least 25 per cent of the shares or voting rights
- Names of all authorised signatories
- Nature and details of the business
- Whether the customer conducts business with any countries subject to national or international sanctions
- Source of funds
- Copies of recent financial statements.

Verification:

1. Identity of business (e.g. relevant company registry search, or certified copy of certificate of incorporation/partnership deed/business registration certificate (or equivalent) or other equivalent independent and reliable sources. The guiding principle is that the documents used have been issued by a government, government body or agency or accredited/regulated industry body. For corporate documents, certification can be by an appropriate authority of the customer (e.g. the company secretary).

2. Identity of one controlling director (e.g. managing director), partner or proprietor (see 'Officers of corporations', below).

3. Identities of all significant beneficial owners owning at least 25 per cent of the shares or voting rights.

4. Authority of authorised signatory(s) to open and operate the account (e.g. board resolution/mandate).

5. Where the shareholders are not natural persons, the structure should be investigated until the natural persons or a publicly listed company are identified. It should then be established whether any such natural person(s) hold a proportionate interest of 25 per cent or more of the customer or exercise management control over it (i.e. significant beneficial owners).

6. Companies with an unduly complex structure of ownership should be subjected to EDD. This generally means there are three layers or more layers of shareholding ownership between the company and the ultimate principal beneficial owners.

For company officers

Identity and due diligence information:

- Full name
- Current residential address
- Date of birth
- Nationality
- Identity document number
- Nature and details of the business/occupation/employment.

Verification:

The preferred document to verify identity would be a government issued document which contains the name, an evidencing photograph or similar safeguard and either the residential address or date of birth. For example:

- passport
- driving licence
- national identity card or
- Electoral ID card.

Enhanced Due Diligence (EDD)

As for NDD, except

1. Verify the identities of two controlling directors (or equivalent) that must include the managing director or CEO.
2. In addition, fuller investigations into the nature of the entity's business, and the legitimacy of its business activities and revenues/sources of wealth and funding. (Corroboration of source of wealth could be from actual documents provided by the customer (e.g. the proof of a sale of a property), available public information surrounding the individual or, where appropriate, from a detailed due diligence report of the relationship manager that has included elements of external enquiry and detailed meetings with the customer.)

These tools are really nothing more than a more detailed, granular manifestation of the 'digging holes' graphic shown in Figure 4.4. If you look at it, you'll see that for SDD there is a relatively light amount of information and verification required, but that these requirements increase as the risk classification rises up through NDD and into EDD. Similarly, detailed tools should exist for each of the customer categories outlined above.

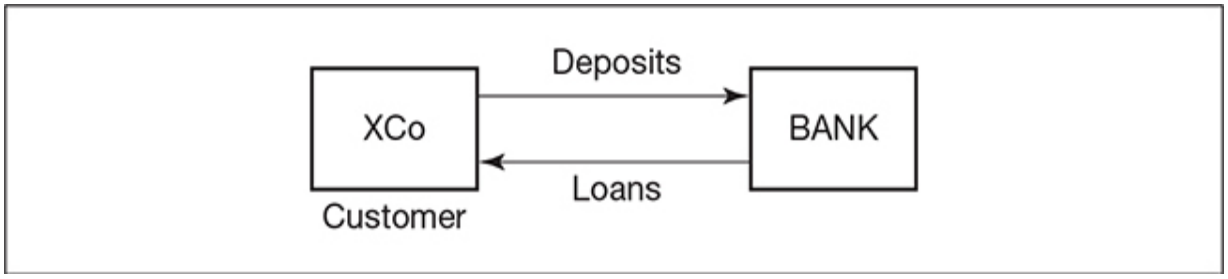
EXAMPLE RISK ASSESSMENT FRAMEWORKS

Constructing a CDD framework for corporate/wholesale banking business

Given the complexity of many modern financial transactions and structures, it may not be immediately clear to your staff who the corporate customer actually is, and so this is something which will need to be spelled out in your policy documents and your training.

Who is the customer? In the type of relationship depicted in Figure 4.6, the answer is straightforward. The customer is a company called XCo that is placing deposits with and taking loans from the bank. However, things may not always be so obvious, so here are a few examples of different types of financial transactions which could be included in policy documentation to guide staff on 'Who is my customer?'

Figure 4.6 **'Plain vanilla' banking relationship**



Example

Case 1

AlnaBank buys from KBank the loan portfolio of WonderTaste Limited, which is in financial difficulties and requires a debt restructuring which KBank is not prepared to provide. According to the workout deal, in addition to acquiring the existing loans, AlnaBank is also to provide an additional credit line of $20 million.

KBank and WonderTaste are both clearly candidates for CDD. But which of these should the CDD be conducted against, or is it both?

The answer in this case is that CDD must be conducted against both counterparties, KBank and WonderTaste. AlnaBank is receiving and paying for financial assets from KBank, and WonderTaste will actually be opening accounts and (hopefully) repaying loans.

Case 2

The hi-tech fund of AlnaBank Growth Ventures Limited (AGVL), - AlnaBank's private equity arm, receives funds from X Limited, Y Limited and Z Limited and invests them in Advance Software Limited, so as to acquire a 65 per cent stake.

The candidates for CDD then are, respectively, X Limited, Y Limited, Z Limited and Advance Software Limited. But against which one should AlnaBank conduct CDD?

The answer in this case is that CDD must be conducted against X Limited, Y Limited and Z Limited since they are the entities from whom funds are being received as part of the investment process. Normally there would be no requirement to conduct due diligence against investee companies such as Advance Software Limited, nevertheless AGVL would be wise to undertake integrity checks against Advance Software before making the investment (see Chapter 5 on managing reputational risk).

Case 3

Joyful Bank, Beijing branch, sets up SWIFT and tested telex arrangements with AlnaBank in India, which are also to be utilised by Joyful Bank's New York and London branches. Joyful Bank is incorporated in the People's Republic of China.

The possibilities for CDD here, therefore, are the three different branches of Joyful Bank in Beijing, New York and London. Against which must - AlnaBank conduct CDD?

The answer here (in the absence of more stringent local requirements or separate subsidiary status for each branch AlnaBank would need to check) is that Joyful Bank would constitute a single legal entity, and as such CDD need only be conducted against that entity, i.e. there would be no requirement to conduct individual due diligence against each of the overseas branches.

Case 4

AlnaBank sells corporate bonds issued by Timeless Textiles to Excel Investments Limited, an investment firm. AlnaBank purchased the bonds in the secondary market from Alpha Investments Co Limited.

AlnaBank could conduct CDD against Timeless Textiles, Excel Investments or Alpha Investments. So against whom is CDD required?

The answer in this case is that CDD must be conducted by AlnaBank against both Excel Investments and Alpha Investments, as the subsequent purchaser and initial seller, respectively, of the bonds in question. This is because there is a direct business relationship between AlnaBank and these two entities involving the receipt of funds (from Excel Investments) and assets with value (from Alpha Investments). There is no requirement for AlnaBank to conduct CDD against the initial issuer, Timeless Textiles, because there is no business relationship between the two.

Case 5

The Habibian Brandy Company in Yerevan, Armenia, is exporting brandy to Party Pubs Limited in Thailand. AlnaBank is advising a letter of credit issued by Thailand Bank on behalf of Party Pubs Limited.

CDD would be possible against The Habibian Brandy Company, against Thailand Bank and against Party Pubs Limited. Against whom should AlnaBank conduct its CDD?

The answer in this case is Thailand Bank, since according to the structure of such transactions, Thailand Bank will have instructed AlnaBank, which will be receiving funds from it. There is no customer or other business relationship between AlnaBank and either the Habibian Brandy Company or Party Pubs Limited which, although lying at the commercial heart of the transaction, are not customers of AlnaBank. However, applying risk-based principles, limited due diligence such as media searches should be considered against these non-customer third-parties as well as name screening.

Case 6

AlnaBank is the receiving bank on a rights issue being arranged by another bank on behalf of its client, Alpha Limited. In the opening stages of the issue, the following applications are received:

Applicant name	Amount ($)
X Limited	300,000
Y Limited	70,000
Mrs Z	5,000

CDD would be possible against all three of the above, but against whom should AlnaBank conduct it? The answer in this case would be X Limited and Y Limited, but not Mrs Z. Why? Because these are one-off transactions and if the issue were oversubscribed, AlnaBank would have to return X Limited's and Y Limited's subscription funds which in each case would be above AlnaBank's maximum threshold for conducting one-off transactions without undertaking customer due diligence. This, of course, would be a potential form of money laundering.

CDD is not required in this case against Mrs Z, however, since the funds which would have to be returned to her in the event of an over-subscription

would be below the relevant threshold.

In this case, no CDD would be required against Alpha Limited either, since according to the structure of such transactions, AlnaBank would have no direct business relationship with Alpha Limited as the issuer.

Note: had X Limited's and Y Limited's funds come from accounts which they held at regulated financial institutions in countries which AlnaBank deemed to have a good, strong AML regulatory framework, then it would be entitled in its policies to rely on the CDD conducted by those financial institutions (as permitted under Recommendation 17 of the FATF standards). However, AlnaBank would have to satisfy itself that copies of relevant documentation would be available immediately upon request. It should also bear in mind that, notwithstanding its operation of such 'reliance' provisions, it would still remain legally responsible for any negative outcome.

Case 7

AlnaBank is the lead manager in the syndication of a loan to Vessyan Textiles, a listed company. The other syndicate banks are Blue Bank, Green Bank and Yellow Bank.

CDD is possible against Vessyan Textiles and the syndicate banks, so against whom should it be conducted?

The correct answer is Vessyan Textiles, which is actually entering into a transactional relationship with AlnaBank. No CDD is required against the syndicate banks since, according to the structure of a syndicated transaction, they do not enter into a transactional relationship with AlnaBank. However, again on risk-based principles, some limited due diligence (name screening and adverse media searches) should be considered on the other members of the syndicate.

Risk-classifying corporate clients: example methodology

Having decided against whom we need to carry out due diligence, before we can determine what level of information and verification is required, we need a practical methodology for classifying clients as either SDD, NDD or EDD. Such a system:

- should be policy-based, such that decisions made about individual relationships can be referred back to a policy document
- should be capable of being operated by the business units themselves, only requiring separate input from your AML specialists in circumstances required under the policy or in difficult or borderline cases where staff are unclear, and
- must be reasonably robust and flexible, in the sense that it covers multiple different scenarios and is responsive to business needs (while, of course, meeting the compliance standards which have been determined).

Corporate banking risk calculator tool

Applying the above, therefore, you need to have a methodology for calculating the appropriate CDD risk level in a relationship which is based on the principles which we have been discussing, and which utilises the country and business sector risk tools described earlier – see Table 4.6.
What the calculator does for business units, therefore, is to provide a - systematised, process-driven way to arrive at a reasoned risk assessment, all else being equal. This last caveat is important because other policy factors will need to be taken into consideration in arriving at the classification. These are dealt with below. It is also important to remember that such processes must be subject to human overview and the application of common sense.

EDD factors checklist

The following example framework is robust, albeit quite simple (it is possible to construct more complex and sensitive frameworks). Under this framework, relationships are classified for business reasons in the lowest level possible for the perceived business risks which they present. The

presence of one or more factors determines that some relationships must always be classified as EDD. These are:

- PEPs, or customers linked to PEPs (unless, for example, the PEP is a non-executive director from a low-risk jurisdiction and does not own or control 15 per cent or more of the customer)
- entities involved in gambling/casinos
- entities involved in the arms trade
- entities dealing with diamonds and other precious stones
- offshore trusts
- entities with complex ownership structures (e.g. three or more layers of ownership)
- entities that issue bearer shares (that is, shares of which ownership passes through physical possession of share certificates).

Table 4.6 **A corporate banking risk calculator tool**

Country risk (country of incorporation or country that customer is operating in, whichever is higher)	Business type (see example business type risk)	Business age 0–1 years = High 1–5 years = Medium Over 5 years = Low	Risk category
High	High	H	EDD
		M	EDD
		L	EDD
	Medium	H	EDD
		M	NDD
		L	NDD
	Low	H	NDD
		M	NDD
		L	NDD
Medium	High	H	EDD
		M	EDD
		L	NDD
	Medium	H	NDD
		M	NDD
		L	NDD
	Low	H	NDD
		M	NDD
		L	NDD
Low	High	H	EDD
		M	NDD
		L	NDD
	Medium	H	NDD

		M	NDD
		L	NDD
	Low	H	NDD
		M	NDD
		L	NDD

In other words, where any single one of the above features is present in the relationship, that relationship must be classified as EDD, notwithstanding the presence of multiple, other, low-risk indicators.

SDD factors checklist

Relationships which can be classified as SDD (unless any of the compulsory EDD features are present, or there is too great a preponderance of other high-risk features) are relationships with corporate entities that are:

- publicly quoted companies or their subsidiaries listed on a well-regulated stock exchange
- companies subject to statutory licensing and industry regulation from low- or medium-risk jurisdictions
- government-owned and controlled bodies from low- or medium-risk jurisdictions.

Again, the presence of one or more of the compulsory EDD features in any of the above relationships would mandate an EDD classification.
In all other cases, according to this framework, you would use the corporate banking risk calculator, the country risk list and business sector risk tools described earlier, in order to arrive at the appropriate risk classification for customers. You would then use the relevant CDD documentation tool to designate in each case what the specific information and verification requirements were for each customer.

Matching information and verification intensity/depth to risk classification

As we saw earlier, the information-seeking and verification activity which you undertake on a relationship should become deeper and more intense as

the perceived level of risk rises. The greater the risk, the deeper you need to dig.
We also looked at a range of different types of information relating both to natural persons in corporate roles (directors and officers of legal entities) and to the entities themselves, and the various methods by which such information could be verified.
The CDD documentation tool can be used in order to assign reasonable and appropriate information and verification requirements to the different risk classification categories (SDD, NDD and EDD) for corporate/wholesale banking customers.
Taking all of the above into account, you should now be able to assign a risk classification to different relationships and allocate appropriate CDD requirements to them. So here are some example cases on which to try out your CDD skills.

Case 1 – Ace Construction Limited

Ace Construction Limited is registered in your country and doing business there, specialising in so-called 'intelligent' buildings. Through a recently won large new contract, it is also doing business in Nigeria. The company was founded six months ago by directors and shareholders (who are also the beneficial owners) David Harman and Peter Markin on the back of two initial, specialist, small office construction contracts undertaken for a Nigerian company which wants to use the technology in their new head office building. Herman Taylor, a local lawyer, holds a power of attorney and is also an authorised signatory.
What risk classification would be appropriate for this relationship and what CDD information and verification should be obtained?
The answer in this case is that this is an EDD classified relationship. From the facts, we can determine immediately that it cannot be an SDD account because it does not fulfil any of the criteria for SDD status that we outlined earlier (it isn't publicly quoted, it isn't subject to statutory licensing and it isn't government-owned or controlled). We also know that it doesn't have to be EDD, because none of the features triggering mandatory EDD status are present (there are no PEP connections, the company is not involved in the gambling, armaments or diamond/precious metals trade, it is not an offshore trust, it doesn't issue bearer shares and it doesn't have a complex ownership structure, as defined). Since it cannot be SDD and need not be EDD,

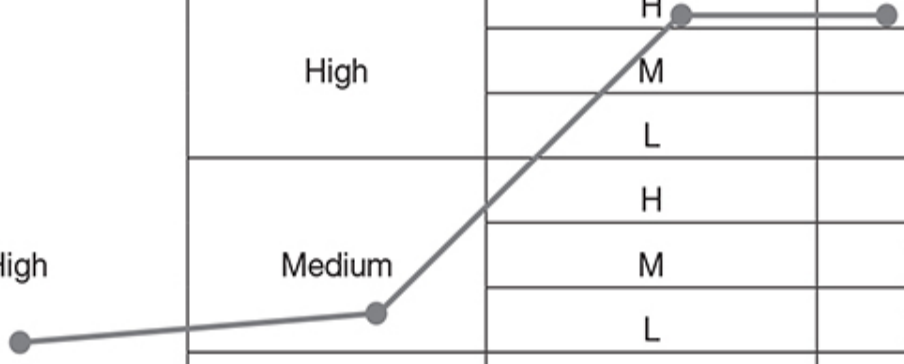
therefore, it could be either NDD or EDD and to determine this we refer to the corporate banking risk calculator. The relevant criteria for using this calculator are country risk (Nigeria = high: remember that the country risk will be the higher of the place of incorporation and place of business, if different), business sector risk (construction = medium) and business age (less than one year = high), according to which the overall classification using the calculator comes out at EDD, as shown in Figure 4.7.
In terms of the information and verification requirements, if we look at the CDD documentation tool we can see that the CDD requirements for this business in the EDD section would therefore be as follows.

Company information

- Full name
- Company number or taxpayer identification number
- Registered office
- Business address (if different)
- Purpose and reason for establishing the relationship
- Expected account activity
- Names of all directors and beneficial owners owning or controlling 15 per cent or more of shares or voting rights
- Names of all authorised signatories
- Nature and details of the business
- Whether the company conducts business with sanctioned countries
- Source of funds
- Copies of recent financial statements.

Figure 4.7 **Application of risk calculator tool to Ace Construction Limited**

Country risk (country of incorporation or country that customer is operating in, whichever is higher)	Business type (see example business type risk)	Business age 0–1 years = High 1–5 years = Medium Over 5 years = Low	Risk category
High	High	H	EDD
		M	EDD
		L	EDD
	Medium	H	EDD
		M	NDD
		L	NDD
	Low	H	NDD
		M	NDD
		L	NDD



Verification of company information

- Certified copy of certificate of incorporation
- Certified copy of search at Companies Registry revealing identities of shareholders and directors
- Detailed investigation into the nature of Ace Construction Limited's business, the types and identities of contracts under which it has earned revenue (and the legitimacy of those contracts), i.e. source of wealth checks, corroborated by information from sources outside of, and independent from, the company.

Personal information

For each of the directors/shareholders David Harman and Peter Markin, and also for the power of attorney holder Herman Taylor, the following:

- full name
- current residential address
- date of birth

- nationality
- identity document number (passport, tax identification number)
- details of any other occupation or employment.

Verification of personal information

For each of the above individuals, sight of an original passport, driving licence or national identity card, with copies certified and retained on the file.

Case 2 – The Golden Export Company

The Golden Export Company is incorporated and registered in your low-risk country. Founded in 1989, it distributes a variety of general industrial products all over the region to low- or medium-risk countries. Its turnover last year was $10 million equivalent and it has a capital and asset base of approximately $25 million equivalent. The company provides generous funding for sports facilities in deprived local areas and desk research shows it to be well-established with a good reputation.

What risk classification would be appropriate for this relationship and what CDD information and verification should be obtained?

The answer in this case is NDD. None of the requirements triggering mandatory EDD status are present, so while it could be classified as EDD, it does not have to be. None of the factors permitting SDD status are present, so it cannot be SDD. If you look at the calculator, you can see immediately that the country risk is medium, the business type risk is low and the business age risk is low which, if you track it through, comes out at NDD (see Figure 4.8) .

In terms of information and verification, again if you look at the requirements in the CDD documentation tool you can see that they are basically the same as for EDD, with the important exception that it is not necessary in this case to undertake the extensive fuller investigations into the nature of Golden Export's business and the legitimacy of its sources of wealth. It is also necessary to verify the identity of only one of its directors.

Figure 4.8 **Application of risk calculator tool to the Golden Export Company**

Country risk (country of incorporation or country that customer is operating in, whichever is higher)	Business type (see example business type risk)	Business age 0–1 years = High 1–5 years = Medium Over 5 years = Low	Risk category
Medium	High	H	EDD
		M	EDD
		L	NDD
	Medium	H	NDD
		M	NDD
		L	NDD
	Low	H	NDD
		M	NDD
		L	NDD

Case 3 – Aeglis Consulting Limited

Aeglis Consulting Limited (ACL) was founded in the UK in 1977 providing IT consulting services in the UK, Canada, Australia and New Zealand, primarily to government departments and public sector organisations. It was owned and run by the Merrit family until they sold the company in 2009 to Challenge Investments, a private equity group whose chairman, John Sandler, is married to a British cabinet minister, Sarah Patterson. Mr Sandler now sits on the Aeglis board. The ownership structure of the company is shown in Figure 4.9.

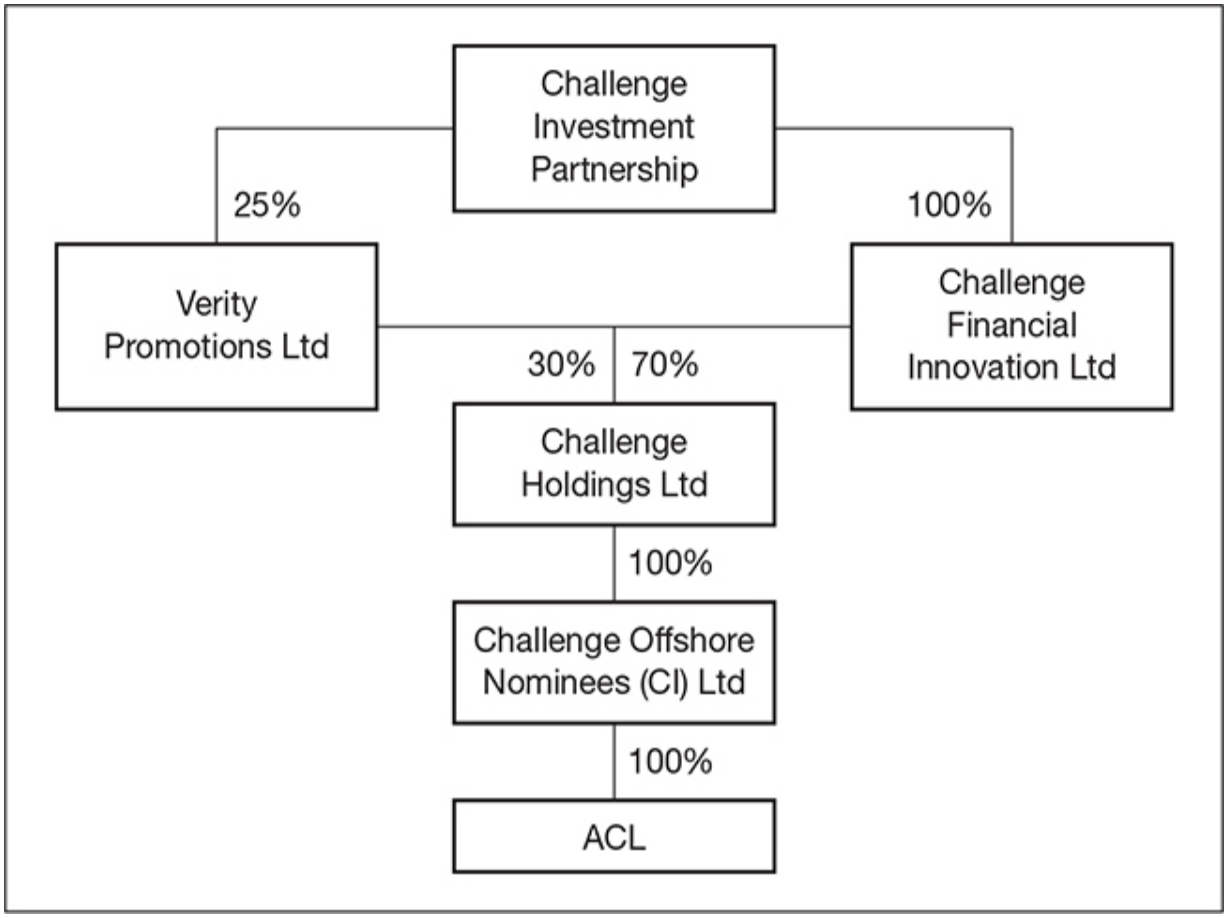
What risk classification would be appropriate for this relationship and what CDD information and verification requirements would apply?

The answer in this case is EDD. This is because notwithstanding the fact that the country, business type and business age risk are all low according to the corporate banking risk calculator, nevertheless the Aeglis Group is

linked to a PEP (its chairman, John Sandler, is married to a UK cabinet minister) and PEP linkage is one of the triggers for automatic EDD status in the example policy framework outlined earlier. In addition, the ownership structure counts as a complex one, being four layers deep, and that is another trigger for automatic EDD status.

From a practitioner's perspective, however, there are at least a couple of features about this potential relationship which mark it out as a 'deceptor'. A deceptor is an account or relationship with many of the hallmarks of low risk, yet which is in fact high risk. The two features of particular concern here are:

Figure 4.9 **Ownership structure of Aeglis Consulting Limited (ACL)**



1. *A recent change in ownership*. Even a business which has been in existence for 35 years can be used for money laundering, if brand new owners decide that that is what they are going to use it for. The historic activities of the company in servicing government departments in and from low-risk countries might have become just that – historic – when the new owners took over in 2009.
2. *The ownership structure*. If you look carefully at the ownership structure you can see that the Challenge Investment Partnership does not actually own 100 per cent of ACL. Verity Promotions Limited actually owns 30 per cent of it, and Verity Promotions Limited itself is only 25 per cent owned and controlled by Challenge Investment Partnership. So who owns the remaining (majority) 75 per cent stake in Verity Promotions Limited? This would be an important question to answer since, without it, you would be taking on a relationship with an entity (ACL) with a 30 per cent beneficial owner about whom you knew nothing.

In terms of information and verification, therefore, not only would we require all the corporate and personal information and verification described in Case 1 for both ACL, the Challenge Investment Partnership and John Sandler, as well as his source of wealth, but also full details of the business activities and reputation of the Challenge Group and a CDD exercise against Verity Promotions Ltd.

Case 4 – Landisbourne Plc

Landisbourne Plc is an industrial components manufacturing group incorporated in England and registered and quoted on the London Stock Exchange. It has been in existence for more than 100 years. It has a significant export business, both to the EU and the US and to a number of developing countries including South Africa, Nigeria, Brazil and Indonesia.
What risk classification should apply to this potential relationship and what CDD information and verification should be obtained?
The answer in this case is SDD. Applying the framework outlined earlier, none of the criteria triggering mandatory EDD status are present, so the account could be either NDD or SDD. From that framework we also see, however, that SDD can be applied to, among others, publicly quoted companies or their subsidiaries on an approved regulated market. Since the

London Stock Exchange is an approved, regulated market according to our regulated markets list, the relationship can therefore be classified as SDD unless the corporate banking risk calculator indicates EDD status. Checking the relationship against the calculator, you find a high-risk jurisdiction (Nigeria and Indonesia are high risk and would defeat the low-risk status of the UK). But you also find a low-risk business type (manufacturer of industrial products) and a low-risk business age (over five years), so overall the level of risk comes out at NDD. EDD is not mandatory and SDD status can apply in this case, which means that you would arrive at an SDD classification.
In terms of CDD information and verification, reference to the CDD documentation tool reveals that for SDD no personal identification and verification of directors and officers is required. Instead, the following would be sufficient:

Corporate information

- Full name, nature and status of entity (public company)
- Company number
- Registered office in country of incorporation
- Business address
- Purpose and reason for opening the account or establishing relationship
- The expected type and level of activity to be undertaken on the relationship.

Corporate verification

- Copy of London Stock Exchange internet page showing the company as being listed
- Board resolution authorising the opening of the account and the authority of its authorised signatories.

CONSTRUCTING A CDD FRAMEWORK FOR FINANCIAL INSTITUTIONS

Despite the heavily regulated environments in which most of them operate, financial institutions are inherently risky to have as customers. This risk arises because they are not just taking care of their own business; they are taking care of other people's business as well. Like the Trojan horse, what matters about financial institutions is what's inside. A financial institution can have perfectly described AML policies, procedures and internal controls, yet if it has a high-risk customer, product and geographic profile, and a management with little regard for AML matters, cold comfort is had from this.

It is one thing to tick a series of boxes in a questionnaire, confirming that the AML policy of a financial institution business prospect includes provisions on customer identification, customer due diligence, staff training, the reporting of suspicions, etc. What is even more important is the culture and habits of the institution. For example:

- How often are AML policy waivers applied? Most AML policies will contain waiver provisions allowing accounts to be opened before the necessary CDD documentation has been contained; indeed the FATF standards permit this. But such waivers are only meant to operate in exceptional circumstances and for a limited period. Is that the case in the institution you are looking at? Or are waivers being given on multiple accounts on a continuous basis?
- What is the record of senior management over-ruling Compliance? In corporate governance terms most institutions are run by the board of directors, not the Compliance Department. When Compliance makes a recommendation, for example against opening an account, how often are they over-ruled?
- Is there any evidence of management indifference or hostility to AML issues? Some senior managers have been known to imply to business colleagues (but rarely in the presence of the Compliance Department) that when revenue and compliance policy conflict, revenue must always come first, if enough of it is at stake.

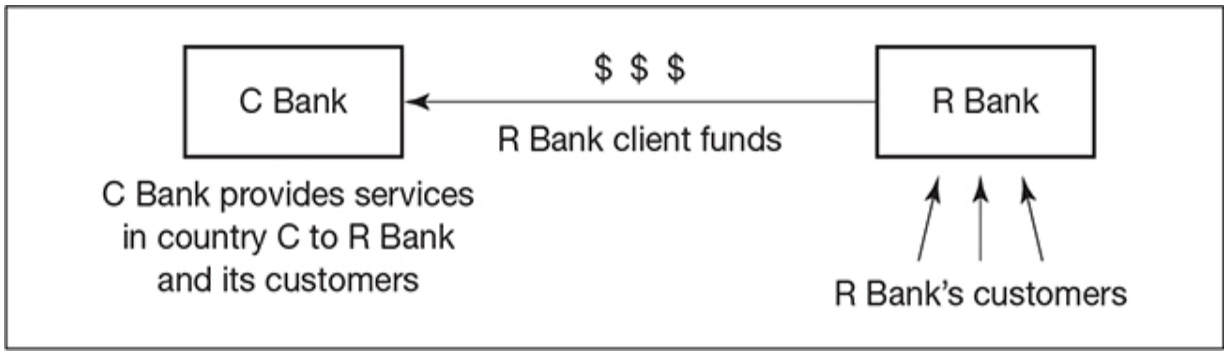
- Is there evidence of a culture of secrecy? For example, are there historic or ongoing issues relating to the management of accounts which no one is prepared to talk about?
- Is there evidence of any re-characterisation of transactions? One way of getting around a compliance or regulatory problem is to make something which is prohibited appear to be something else (something permitted) in the books and records of the institution. Typical examples include misrepresenting the origin of funds, the beneficial ownership of funds and the type and purpose of transactions. In problem institutions staff may know or suspect that there is a problem with what they are doing, but they may also take the view that it is simply 'the way things are done around here'.
- Is there evidence of overly affluent senior management lifestyles or staff remuneration being significantly above the rest of the market? This is a red flag for potential criminal associations in any business, and a financial institution is no different. Consider the following excerpt. It is based on information given to the author from an industry colleague in relation to a visit to a potential respondent bank.

> Our inspection revealed extremely poor levels of AML preparedness . . . Staff had only the most basic levels of awareness. The AML procedures were extremely brief and lacked detail and training appeared to be non-existent. Worryingly, no IT system existed for checking the status of proposed customers against internationally recognised lists of proscribed persons and there appeared to be no systematic monitoring of customer accounts, even relatively high-risk accounts such as non-residents, politically exposed persons and companies domiciled in offshore jurisdictions. Perhaps of most concern were the attitudes displayed by some of the senior managers with whom we spoke, who made no attempt to hide their ignorance of the new legislation and whose concerns revolved mainly around the business they believed they would lose as and when the new controls were applied.

Source: Anonymous

Financial institutions, then, are one of the riskiest types of customers for another financial institution (e.g. your own organisation) to have. This is particularly so when the relationship between the two of you is that of respondent and correspondent (see Figure 4.10) .

Figure 4.10 Correspondent/respondent banking relationship



In the above correspondent banking relationship, C Bank is the correspondent providing services (e.g. clearing and payments services) to R Bank from Country R, which is the respondent bank in the relationship. R Bank is C Bank's customer and C Bank has an obligation to undertake effective due diligence against its respondent. As an industry colleague once commented memorably during an event:

> **'Health-wise, you have to remember that starting a correspondent banking relationship with a new respondent bank is a bit like starting a serious relationship with someone; if they're sleeping around without your knowledge, then you could be in big trouble.'**

It's a situation, therefore, in which you really want to know as much as you can about your new client and the example policy framework which follows is designed to help you achieve that.

Example CCD policy framework for financial institutions

As was the case for the non-financial corporates just discussed, the task is to create a practical, robust system for the risk assessment of financial institution clients which can be implemented by business units directly, only seeking additional guidance in borderline cases or where certain aspects are uncertain.

The default position – EDD

Reflecting the significant areas of risk associated with financial institutions, the example framework described here is one in which the default position for a new financial institution client is a risk assessment classification of EDD. In other words, all financial institution clients will start out as EDD and can only achieve a lower risk classification through the elimination of certain key risk criteria to be described. The more of these criteria which are eliminated, the lower the level of risk classification until one arrives at SDD status, indicative of the lowest levels of risk.

Unacceptable relationships

As with all other customer types, however, the starting point for financial institution customers is unacceptable relationships. Here in our example policy we cite the following blockers, the presence of any of which will prevent the acceptance of the client (i.e. no risk assessment takes place because the client is simply rejected):

- shell banks
- unlicensed banks
- unregulated money service bureaux and crypto exchanges
- entities and individuals subject to UN sanctions
- where connections with money laundering or terrorist financing are suspected
- financial institutions that maintain accounts for customers which are anonymous or which are in obviously fictitious names
- financial institutions that issue bearer shares.

Mandatory EDD status

Under this example framework the presence of any of the following will mandate an EDD risk classification for the financial institution in question:

- There is to be a correspondent relationship with the financial institution (FI):
  - that is a 'downstream correspondent clearer' (i.e. it provides correspondent bank services itself to other financial institutions further down the chain), or
  - whose own customers will have direct access to its account with your bank, or
  - that is a private bank and conducts private banking as its only business.

OR

- the FI is from a high-risk jurisdiction, or
- the FI is a money service bureau and/or crypto exchange, or
- the FI is owned and controlled by a PEP.

If none of the above mandatory EDD factors apply, then in this example framework there are two situations in which an NDD rating is possible, as follows.

Potential NDD status

Situation 1 – No correspondent relationship

- Where there is to be no correspondent/respondent relationship between your institution and the FI under consideration, and
- the FI is regulated in a low- or medium-risk jurisdiction.

Situation 2 – Limited correspondent relationship

- While there is intended to be a correspondent/respondent relationship between your institution and the FI under consideration, nevertheless none of the features triggering EDD status above, are present, and
- the FI is regulated in a low-risk jurisdiction.

Potential SDD status

Following on from the above, under this example framework business units are able to apply an SDD risk classification to a proposed relationship with a financial institution only if:

- there is to be no correspondent/respondent relationship between the financial institution and your bank, and
- the financial institution is regulated in a low-risk jurisdiction.

It will of course be possible to manipulate the above framework either to increase or reduce the risk appetite. For example, additional categories could be added to either or both of the prohibited and/or mandatory EDD lists or NDD could be permitted only in low-risk jurisdictions.

The important thing is that those responsible for CDD in business units are not left making individual, personalised judgements about different prospective accounts according to their own personal perceptions. Individual judgement is, of course, important – but only after an ordered analysis according to established, enterprise-wide principles.

For Financial Institutions a primary requirement of due diligence is to be satisfied as to the quality of their AML/CFT controls.

The type of FI relationship should determine the level of this due diligence and in this regard the latest Wolfsberg standards offer assistance. It will often be the case that while an organisation has correspondent relationship customers, it will itself be a customer of other banks who will require similar due diligence.

As such the Wolfsberg Questionnaires, which have become an international, industry standard, can be completed by the organisation itself to be (a) provided to another FI where they are entering into a relationship as evidence to their effective AML/CFT systems and controls, as well as (b) being requested by an organisation from a potential FI customer.

There are two Wolfsberg Questionnaires; the very detailed Correspondent Banking Due Diligence Questionnaire (CBDDQ), which is for use where correspondent banking relationships are being opened, and the Financial Crime Compliance Questionnaire (FCCQ) where the FI relationship is not of a correspondent nature.

While these questionnaires provide a great degree of detail surrounding the AML/CFT controls of an FI they do not, of course, provide complete

comfort that such controls are actually applied effectively in practice. As such, in the most high-risk relationships it may be prudent to consider a visit to or a detailed discussion with the potential customer FI (either the MLRO or the relationship manager, or both) to satisfy oneself as to the application of those systems and controls.
See https://www.wolfsberg-principles.com/wolfsbergcb

Example cases

As we did earlier for non-financial corporates, let us now test-drive this example policy framework with some case studies. As before, your task is to use the policy principles above, in conjunction with the tools in order to arrive at a risk classification, and CDD documentation and verification requirements for each case.

Case 1 – Ocean Bank

Ocean Bank wants to use your bank as its correspondent in your country. Ocean Bank is incorporated, registered and regulated in the Republic of -Bissan (a made-up country). It is not a money service bureau or crypto exchange, it conducts only wholesale corporate business and the largest shareholder is a UK pension fund with 12 per cent. It has no financial institution clients and its own customers will not have access to its accounts with you.
What risk classification is appropriate and what CDD information and verification requirements would apply?
The answer in this case is EDD. If you check the country risk tool you will see that the Republic of Bissan is classified as a high-risk jurisdiction and regardless of anything else, the incorporation of a potential FI client in a high-risk jurisdiction makes an EDD risk classification mandatory under the example policy framework which we are applying here.
In terms of CDD information and verification, you would look to your CDD documentation tool for financial institutions (EDD section) in order to obtain this. The typical types of requirements would be the following:

Corporate information

- Full name

- Registered number
- Registered office
- Business address
- Purpose and reason for opening account
- Nature of the financial institution's business
- Ownership details
- Assessment of AML controls
- Reputation and quality of supervision as well as details of ownership and executive management.

Corporate verification

- Either a copy of the internet page published by Ocean Bank's regulator, confirming its regulated status, or
- a certified copy of its licence.

No personal identification and verification would be required, given Ocean Bank's regulated status. However, significant due diligence would have to be undertaken concerning Ocean Bank's AML policies and controls, as well as its reputation and underlying business, its ownership structure and any natural persons with significant beneficial ownership or control, along with the names and reputations of its senior executive management.
In this regard, the important additional tool would be a questionnaire designed to elicit information regarding Ocean Bank's AML controls based on the Wolfsberg CBDDQ. An example of such a questionnaire is presented in the Appendix. Given the heightened risk of Ocean Bank, consideration should be given to testing the effectiveness of the Bank's control through a visit/discussion with appropriate Ocean Bank people (MLRO/RM or both).

Case 2 – Haptan (TCI) Bank

Haptan (TCI) Bank, incorporated, registered and regulated in the Turks & Caicos Islands, wishes to open correspondent accounts with your bank. Haptan (TCI) Bank is a wholly-owned subsidiary of Haptan Bank, which is incorporated, registered and regulated in Bulgaria. Haptan (TCI) does not conduct private banking business, will not be allowing customers direct access to its accounts with your bank and will not have any financial institution clients of its own. It is not a money service bureau or crypto exchange.

What risk classification would be appropriate and what CDD information and verification requirements would apply?

The answer in this case is NDD, but with a caveat. None of the criteria for mandatory EDD status is present, so Haptan (TCI) does not have to be classified as EDD. It cannot be classified as SDD because there will be a correspondent banking relationship if the account is accepted. Looking at the two situations for NDD, you can see that one of them applies, i.e. where the proposed correspondent/respondent banking relationship would not involve downstream correspondent clearing (Haptan (TCI) Bank has no financial institution clients) or access by Haptan (TCI)'s own customers to its account with your bank. Haptan (TCI) Bank is also regulated in Bulgaria which is a member state of the EU and is therefore subject to the EU Directives. The account would be eligible, therefore, for NDD status.

But should it be thus classified? If you look again at the fact pattern you can see that there are in fact several indicators of higher risk. Notwithstanding the huge strides made by many EU 'accession states' (ones which joined after 2000, having formerly been part of the old Soviet bloc) in bringing their AML laws into line with the standards required by EU membership (Bulgaria included), financial institutions are still entitled to draw their own conclusions and many would take the view that a risk premium should apply in the case of some accession states, as they continue their fight against organised crime and political corruption. The area of south-east Europe (the Balkans) of which Bulgaria forms a part has, in recent decades, developed an unwanted reputation for its associations with corruption (e.g. see https://www.gfintegrity.org/is-bulgaria-losing-the-war-on-corruption/) and with organised crime, particularly people trafficking for modern slavery. The Turks & Caicos Islands are medium-risk rather than low-risk in the example country risk tool, as well as being an offshore jurisdiction. So you might want seriously to consider EDD status, at least initially, as well as a due diligence visit to the bank to provide further comfort on actual *de facto* compliance with policies.

In terms of CDD documentation and verification, therefore, the same requirements would apply as in Case 1 above, with the exception that evidence of the majority ownership by Haptan (TCI) Bank would have to be obtained, as well as further and deeper enquiries recommended above.

Cases such as this prove the importance of standing back at the end of a standard process and actually thinking about the risks, rather than just

applying a ‘tick-box’ approach and going with whatever result comes out. Ask yourself, despite the fact that the policy framework would permit you to accept the client on this basis, would you really be comfortable doing so, and if so, after what enquiries?

Case 3 – Blossom Bank of Tokyo

Your bank is setting up bilateral, tested, telex arrangements with Blossom Bank of Tokyo, established, registered and regulated in Japan. Blossom Bank is not a money service bureau or crypto exchange and does not have PEP ownership or control.

What risk classification would be appropriate and what CDD information and verification requirements would apply?

The answer in this case is SDD for financial institutions. None of the criteria for mandatory EDD status are present, the relationship is not to be one of correspondent/respondent and a look at the country risk tool reveals that Japan is an equivalent jurisdiction. So SDD is possible, and an overall look at the fact patterns does not reveal any other less obvious high-risk indicators, which means that an SDD risk classification would appear to be appropriate.

The CDD documentation requirement here would probably be: full name, registered number, registered office in Japan, business address and the purpose and reason for opening the account (although this seems pretty clear from the description provided). Verification would simply be to establish the regulated status of Blossom Bank in Japan by a recognised method (e.g. a printout from the relevant page of the Central Bank of Japan referring to Blossom Bank as a regulated entity). Note that with SDD there is no requirement to investigate the AML controls of the financial institution nor its business, underlying activities, customer base or ownership. Given that this is not a correspondent banking relationship, a CBDDQ would not be necessary, but a completed Wolfsberg-style FCCQ would be appropriate.

CONSTRUCTING A CDD FRAMEWORK FOR RETAIL/CONSUMER BANKING BUSINESS

In most institutions retail/consumer banking will constitute the business area in which the greatest volume of accounts are being analysed and opened. Potential customers include not only private individuals and family members, but also, in many institutions, small-to-medium enterprises (SMEs) which in some institutions may be managed by the consumer/retail business if they fall below certain corporate banking thresholds.
The purpose of this section is not to suggest how to deal with all possible combinations of eventuality. Rather, it is to get you thinking about how you can construct policy frameworks which allow business units to implement the risk-based approach in practice by utilising relevant criteria such as country risk, product risk and customer type risk.

Example retail/consumer risk assessment framework

Prohibited relationships and screening

As with all other types of business our retail/consumer risk assessment framework must begin with the need to screen all applicants against the institution's alert list of proscribed entities. There will then be those categories of relationship which it is your policy not to do business with. We shall assume for these purposes that the list of unacceptable relationships is the same as for the corporate side of the business, i.e. shell banks, unlicensed banks and unregulated money service bureaux and crypto exchanges, customers subject to UN sanctions or where money laundering or terrorist financing are suspected, and anonymous accounts or accounts in obviously fictitious names.

CDD risk classification principles

Generally, simplified due diligence is not appropriate for individuals and is not therefore permitted. Therefore, the risk classification categories that we are dealing with are EDD for the higher-risk accounts and NDD for lower-risk accounts.

Mandatory EDD status

As with corporate banking business, in this consumer/retail framework the following would trigger mandatory EDD status:

- all accounts linked to PEPs (except where the PEP is a government appointee in a state-owned company and is not a significant beneficial owner in that entity)
- money service businesses and crypto exchanges.
- gambling and casino entities
- entities issuing bearer shares
- complex structures of four or more layers of ownership.

Different organisations structure their retail business differently and it may be that they allow SMEs (small-to-medium enterprises) as part of their retail portfolio, or not. This should be clearly understood and agreed as the SME segment can be, as a general rule, a higher-risk segment in its own right, sitting alongside a large, low-risk (individuals) segment. This is why the EDD factors above *may* apply even in a retail segment. Where this is the case, care must be taken to ensure the appropriate risk mitigation measures are in place for not just CDD but also training, assurance/audit testing and transaction surveillance.

Determining the difference between EDD and NDD

If a retail/consumer relationship does not need to be classified as EDD, then you must determine whether it should be EDD or whether it can, in fact, be NDD. In this example framework we take a modified approach and the relevant factors for making that decision are as follows:

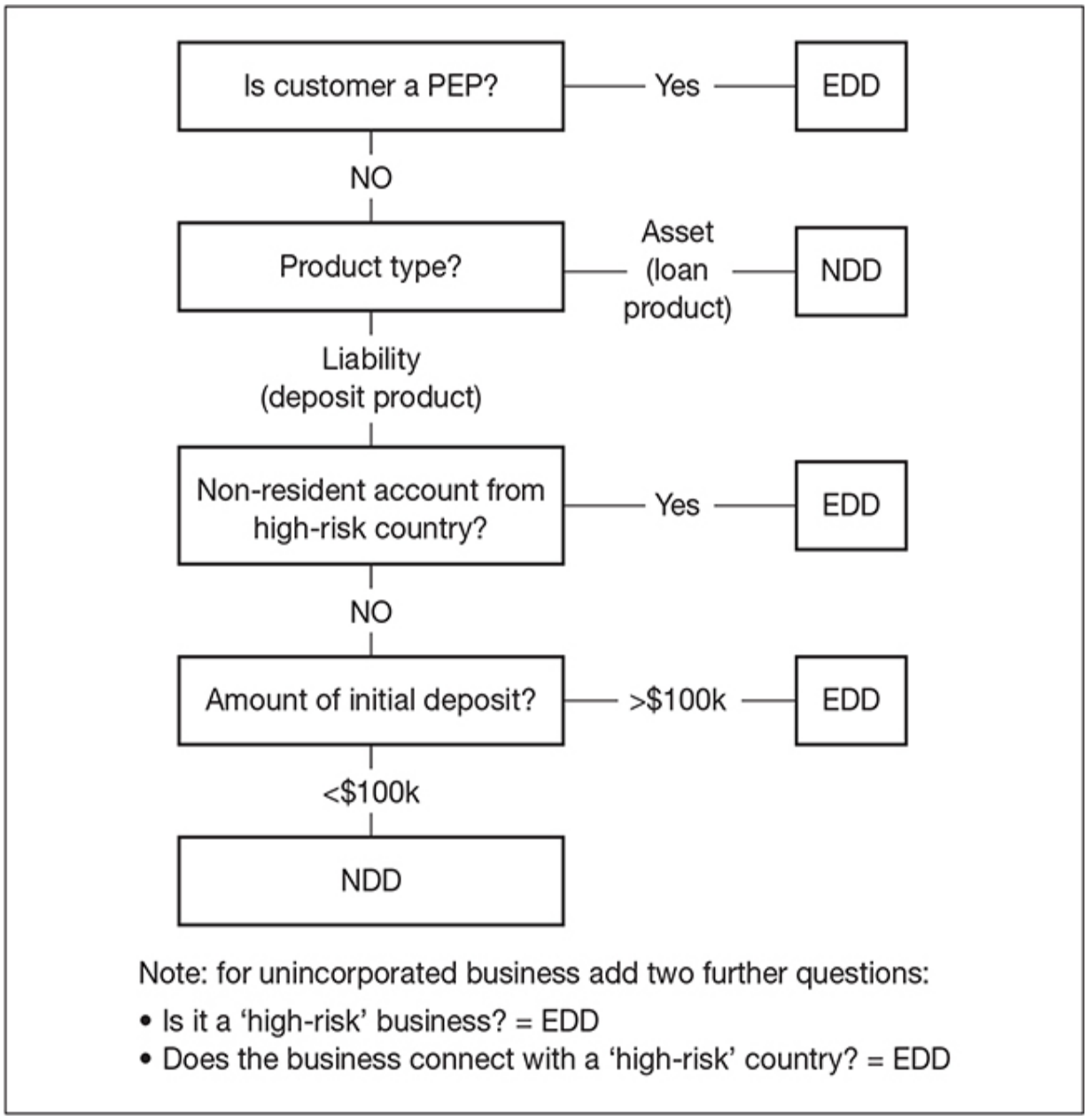
- Product type – i.e. whether it is a liability product such as a deposit product (typically indicative of higher risk) or an asset product, such as a loan product (typically – though not always, as we shall see – indicative of lower risk).
- Geography – whether the relationship will entail the opening of a non-resident account from a high-risk country.
- The amount of the opening deposit – deposits above a certain threshold would indicate higher levels of risk, below that threshold would indicate lower levels of risk.

Figure 4.11 suggests a practical framework in which such criteria could be made to work. It contains a series of questions relating to the key criteria, the answers to which determine whether or not a prospective relationship is classified as either EDD or NDD. Answers indicative of lower-risk levels point the decision towards NDD, and vice versa for EDD.

So as long as the customer is not a PEP or linked to a PEP (something which triggers automatic EDD status) then if the proposed product is an asset (loan) product, the classification can be NDD.

In the case of liability (deposit) products, if the customer is from a high-risk country, opening a non-resident account, then again the status will be EDD. Even if the account is a domestic account or a non-resident account from a medium- or low-risk country, then the account will still be assessed as EDD if the amount of the initial deposit exceeds $100,000.

Figure 4.11 **Example retail banking risk assessment framework**



If the customer is opening a domestic account, or is based in a medium-or low-risk country and opening a non-resident account from there, and the amount of the initial deposit is less than $100,000, then the account may be rated as NDD. Remember that an SDD rating is not permissible for individuals.

Under this example framework there are two further risk assessment considerations for unincorporated businesses (such as, for example, where a private individual or individuals are opening an account for a trading business that they run). If the business type is high risk (according to the

business type risk tool) or if it is connected with a high-risk country (according to the country risk tool) then it must be rated as EDD.
Let's now put this example framework into practice with some case studies.

Case 1 – Sophie Marsal

Sophie Marsal has been posted to your country and wishes to open current and savings accounts with your bank. She presents herself in person at the main branch. She is a French national and will be resident in your country. The initial deposits on her account will be $20,000 or equivalent. She is a senior diplomat at the French Embassy in your country and is noted on your institution's alert list as such.
What risk classification would be appropriate and what CDD information and verification requirements would apply?
The answer in this case is EDD. This is because the prospective customer's PEP status triggers automatic EDD status under the example risk framework. As such, the CDD information required according to any CDD documentation list would probably be along the following lines:

- full name
- current residential address
- date of birth
- nationality
- identity document number
- nature and details of her employment
- the purpose and reason for her wishing to open the relationship
- the source of funds
- the anticipated level and type of activity on the account
- corroboration of her source of wealth.

In terms of verification, her identity would need to be verified either through an official document such as her passport, national identity card or driver's licence, with certified copies retained on the file.

Case 2 – Mr and Mrs John Vangora

Mr John Vangora wishes to open a joint current account with your bank. He is an electrician and his wife, Maria, works in a shop as a supervisor. They

are local residents who plan to deposit $11,000 initially as well as taking out a home improvement loan for $7,000 to be repaid over five years.
What risk classification would be appropriate and what CDD information and verification requirements would apply?
The answer in this case is NDD. None of the triggers for mandatory EDD status are present (they are neither PEPs nor operating any high-risk businesses, they are not non-residents from high-risk countries and the proposed amount of their deposit is well below the $100,000 threshold). Nothing else about the case indicates higher levels of risk so an NDD classification is both correct and appropriate.
In terms of CDD information and verification, the requirements according to the CDD documentation tool would be as for the applicant in the previous case, except without the requirement to investigate and corroborate their sources of wealth. An important point to note is that since the account would be a joint account, identification and verification would need to take place for both Mr and Mrs Vangora. Any document verifying their address would need to be addressed to both of them, or separate documents would be required for each.

Case 3 – John Fantwe

John Fantwe is a financial consultant resident in Abuja, Nigeria. He travels to your country on a frequent basis for business purposes and wishes to open both a current account and to obtain credit card facilities. He indicates that because he anticipates having heavy expenditure requirements in the few months following the opening of his account, he will fund it initially with $180,000 coming from his bank in Nigeria.
What risk classification would be appropriate and what CDD information and verification requirements would apply?
The answer in this case is EDD. Applying the customer profile against both the policy requirements for mandatory EDD status and the flowchart in Figure 4.11, you can see that two features necessitate EDD status. First, the fact that Mr Fantwe is a resident of a high-risk jurisdiction (Nigeria) opening a non-resident account, and second, the amount of the initial deposit, which exceeds the $100,000 threshold stated in the flowchart.
The CDD information and verification requirements, therefore, would be as for the first case involving the PEP, Sophie Marsal. It would be important to determine exactly what type of financial consultant Mr Fantwe was and, in

particular, whether any of his clients were PEPs or other high-risk individuals in his own country. Financial consultants and other types of agents and financial representatives acting as facilitators and middle-men for the movement and placement of funds obtained through corruption and state theft, for example, is a known route for money laundering and you would therefore have to be pretty certain about every aspect of Mr Fantwe's business before the account could be opened, even with its EDD status. This level of research would not be easy, but if you were unable to obtain satisfactory answers you could not open the account. In this regard you would deploy the source of wealth questionnaire tool shown earlier in this chapter.

CONSTRUCTING A CDD FRAMEWORK FOR PRIVATE BANKING

For the reasons discussed in the previous chapter, private banking and wealth management business entails money laundering risks which are higher than those for regular consumer and retail banking. Accordingly, use of a standard retail/consumer risk assessment framework will often be inappropriate. The framework for private banking needs to be more detailed and to contemplate a greater range of account activity.

Example private bank risk assessment framework

Prohibited relationships

- Shell banks, unlicensed banks and unregulated money service and crypto exchange businesses
- Companies issuing bearer shares
- Wealth derived from prohibited business
- Subject to international sanctions or on a list of prohibited individuals/entities
- Convictions for specific criminal charges and/or activities inconsistent with your institution's policies and values

- Anonymous or numbered accounts
- Direct access to any concentration accounts (basically an account that commingles funds from multiple different beneficial owners).

For all other relationships

In the example framework shown in Figure 4.12 you again see a prohibited client list leading to automatic account refusal and a list of features leading to automatic EDD status. However, in comparison to the retail/consumer framework, the simple asset product vs liability product combined with initial deposit amount methodology is replaced with a product risk methodology based on cash transactions and cross-border wire transfers, combined with a country risk vs customer business type risk matrix similar to that used in the corporate risk assessment framework.

In particular, this framework does not envisage automatic NDD status for loan accounts, but rather looks at the volume of activity on accounts (in and out) via either cash or overseas wire transfer payments.

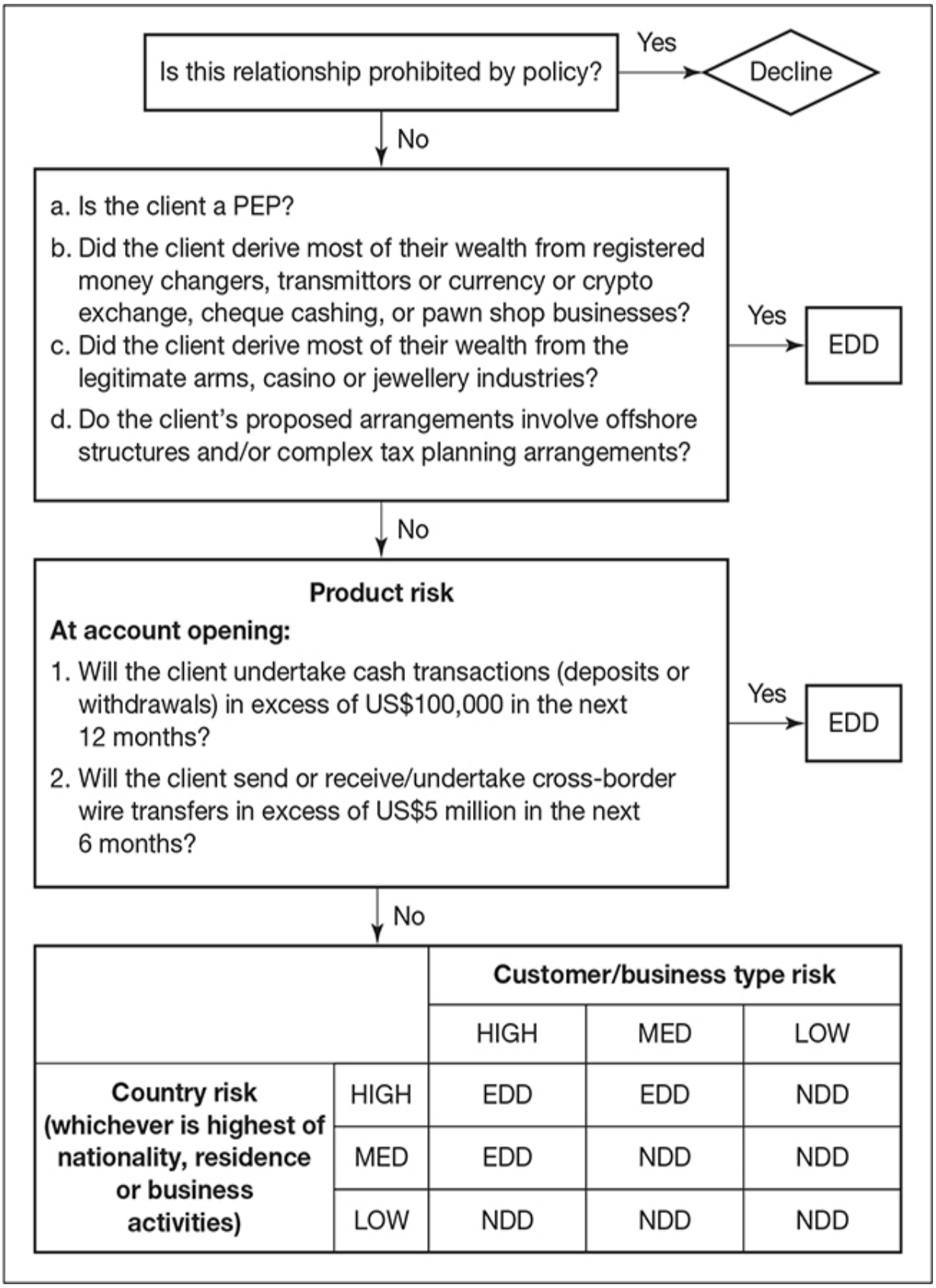
In addition, there is an expanded list of prohibited relationships which now includes both 'convictions for specific criminal charges and/or activities inconsistent with our policies and values' and direct access to concentration accounts. This is an appropriate expansion, given what we know about the types of personalities who often use private banking services and the notorious misuse of some private banking secrecy products (such as concentration accounts) in reported cases.

As before, we can try out this example framework with some examples.

Case 1 – Wolfgang Hamann

Wolfgang Hamann is a German expatriate living in your country. His significant wealth derives from his family's business in the retail sale of pharmaceutical and medical products mainly in the EU, but also in China. Hamann International GMBH has been publicly quoted on the Frankfurt Stock Exchange since 1998 but Mr Hamann is still a significant shareholder in the company and sits on its advisory board. He is interested in deploying some of his capital towards high-risk investments and to that end he is going to make $3.75 million available through an investment account, with instructions to focus on China. Internet searches reveal no allegations of criminality or nefarious activities.

Figure 4.12 **Example risk assessment framework for private banking/wealth management**


Is this relationship prohibited by policy?
Yes
Decline
No
a. Is the client a PEP?
b. Did the client derive most of their wealth from registered money changers, transmittors or currency or crypto exchange, cheque cashing, or pawn shop businesses?
c. Did the client derive most of their wealth from the legitimate arms, casino or jewellery industries?
d. Do the client's proposed arrangements involve offshore structures and/or complex tax planning arrangements?
Yes
EDD
No
Product risk
At account opening:
1. Will the client undertake cash transactions (deposits or withdrawals) in excess of US$100,000 in the next 12 months?
2. Will the client send or receive/undertake cross-border wire transfers in excess of US$5 million in the next 6 months?
Yes
EDD
No

		Customer/business type risk		
		HIGH	MED	LOW
Country risk (whichever is highest of nationality, residence or business activities)	HIGH	EDD	EDD	NDD
	MED	EDD	NDD	NDD
	LOW	NDD	NDD	NDD

What risk classification would be appropriate and what CDD information and verification requirements would apply?

The answer in this case is NDD. Running it through the example risk assessment framework above, none of the criteria for automatic prohibition are present. Hamann is not a PEP, nor is his wealth derived from automatic EDD businesses (in fact the retail sale of pharmaceutical and medical products is a medium-risk business according to the business type risk tool shown earlier). His wealth is not derived from the arms, casino or jewellery industries and we are not told of any offshore structures or complex tax planning arrangements. In terms of product risk, there are to be no cash deposits or withdrawals, or overseas wire transfers (whether into or out from the account) in excess of the EDD threshold limits stated in the framework.

Looking, finally, at the country risk vs customer/business type risk matrix, you have a country risk rating of medium (remember, the highest of country of residence, nationality or business will prevail, and China is stated in the country risk tool to be medium risk) and the business type risk is medium risk. That comes out at NDD in the matrix shown in Figure 4.13. There appear to be no other significant factors at play and therefore an NDD rating would appear to be appropriate.

In terms of information and verification, a CDD documentation tool for personal accounts would dictate information and verification requirments along the following lines:

Information

- Full name
- Current residential address
- Date of birth
- Nationality
- National identification number/tax identification number
- Nature and details of business/occupation
- Source of funds for account opening
- Purpose and reasons for establishing the relationship
- The anticipated account activity.

Figure 4.13 **Application of risk calculator tool to Wolfgang Hamann**

		Customer/business type risk		
		HIGH	MED	LOW
Country risk (whichever is highest of nationality, residence or investment activities)	HIGH	EDD	EDD	NDD
	MED	EDD	NDD	NDD
	LOW	NDD	NDD	NDD

Verification

- Passport viewed and copy taken
- Supporting document such as a utility bill showing the address
- Evidence of his connection with Hamann International GMBH (e.g. Company annual report).

Case 2 – Yuri Dimitrov

Yuri Dimitrov is the Russian owner of a former state-owned oil company V-Oil. Prior to his acquisition of V-Oil in 1992, Dimitrov's business interests lay in the hotel and leisure industry (specialising in casino resorts), with successful resorts on the Black Sea coast. He was already a multimillionaire at that point, but this was as nothing compared to the wealth generated after the privatisation of V-Oil and his acquisition of a controlling stake in it. He wishes to open dollar and euro accounts with your bank at its branch in -Switzerland with an initial transfer of $10 million. He has no private residence in your country and has approached your private bank on the basis of a personal recommendation from one of his business partners.
What risk classification would be appropriate and what CDD information and verification requirements would apply?

At the level of the central nervous system this case is so obviously EDD as to perhaps make further analysis unnecessary (‘gut reaction’ is, after all, important). Nevertheless, we are in the business of analysing risk, not merely responding to personal instincts, so let us apply the example framework to the case and establish on what grounds this is an EDD situation.

Putting the facts through the flowchart, you can see immediately that since a substantial portion of Mr Dimitrov’s wealth has come from the casino business, then for that reason alone the account would have to be classified as EDD. Even if it were not, the existence of dollar and euro cross-border wire transfer activity in excess of $5 million within a six-month period would necessitate an EDD risk classification. Even if that were not so, then an application of the country risk vs customer/business type risk matrix of ‘high risk’ and ‘high risk’, respectively, would yield an EDD classification.

On these types of cases, however, with these types of potential clients, one also has to look carefully at the reputational risks involved. In particular, the first question in the policy framework relates to whether or not the prospective client is of a prohibited client type. One of the prohibited client types is a person with a conviction for criminal offences and/or a person who is engaged in activities inconsistent with organisational policies and values. We know that the business environment in his country, Russia, during the 1990s was extremely volatile, with business practices (particularly those associated with the privatisation of state-owned industries) that were aggressive, controversial and possibly illegal. We don’t know from the facts as stated whether or not any of this applies to Mr Dimitrov, but we would definitely need to find out. Accordingly, this is one of those instances where the real question for many organisations would not be what risk classification to give to the potential client, but rather whether or not the client should be accepted for a business relationship at all (see Chapter 5 for more information on this).

If you do decide to take Mr Dimitrov on as a client, then the CDD information and verification requirements would be extensive. You would require not only all the NDD information listed in the previous case, but also much more extensive background checks as well as detailed source of wealth information.

5

Reputational Risk

Managing reputational risk

When banks go wrong: cases of punishments and penalties

Managing reputational risk: the experience of the MDBs

The integrity ‘red flags’ checklist and the due diligence investigation tools

Practical application

MANAGING REPUTATIONAL RISK

As we noted at the beginning of the book, money laundering and terrorist financing risks to organisations aren’t just confined to the possibility that your organisation is actually used by criminals and terrorists to launder

money and finance terrorist acts. There is a significant risk to the reputation of your organisation if you are found to have fallen short of the standards which are required of you, and this takes the form of financial penalties, public censure by regulatory authorities and of course negative media coverage.

The UK's Financial Conduct Authority defines reputational risk as:

> **'the risk that the firm may be exposed to negative publicity about its business practices or internal controls, which could have an impact on the liquidity or capital of the firm or cause a change in its credit rating.'**

The US Federal Reserve defines it thus:

> **'reputational risk is the potential loss that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation or revenue reductions (financial loss).'**

Clearly, then, reputational risk involves a potentially uncomfortable meeting point between what you do as an organisation on the one hand, and how people judge what you have done on the other. The way you run your business, the actions you take, the risks you assume, the policies you implement (or don't implement, as the case may be) and the values which you espouse (or say you espouse) must pass the test of third-party opinion, be it shareholders, customers, governments and regulators, politicians, NGOs and pressure groups, your fellow industry players and counterparties, the media, members of the public and – let's not forget this – anyone in possession of a blog, a Facebook page or a Twitter account. In a world of globalised markets, volatile share prices and instant communication, what people think about you and what they are saying about you matters as much as almost anything else you can think of. And when it comes to your dealings with (suspected) criminals, money launderers, terrorists and proliferators of weapons of mass destruction, it's not hard to see how the sensitivities can become extreme.

One of the things the organisation you work for is almost certainly trying to do is to demonstrate to the world that it is an organisation of integrity, one

which they can trust. Failing regulatory tests and engaging in associations with those of a dark reputation are not ways to achieve such an objective.

It's crucial to note here an important distinction, however, which can sometimes be lost in the scramble to reduce reputational risk. Integrity and reputation are *not* the same thing. With professional management of an issue, it's possible to have an excellent reputation while actually being an organisation or a person of very little integrity. This is significant in two respects. First, if your organisation is caught out managing its reputation in this way – enjoying the financial benefits of selective lapses while milking its overall compliance for all it is worth – then the consequences are likely to be much worse. Second, and equally importantly, it must be remembered that customers, too, are aware of the benefits of reputation management and will often employ sophisticated techniques to bamboozle relationship managers and risk functions into thinking that they are a certain type of person when in fact they are the very opposite.

Ideally, therefore, in order to manage reputational risk effectively your organisation requires not only effective policies and controls combined with a genuine determination to apply them at all times (even when there are negative financial consequences to doing so), but also the capability to detect reputation management in applicants for business, and to respond appropriately through effective due diligence.

WHEN BANKS GO WRONG: CASES OF PUNISHMENTS AND PENALTIES

To demonstrate the wide range of areas in which financial institutions have been criticised and sanctioned for failing to meet recognised AML standards, below are brief examples of some major instances in recent years.

Example

HSBC 2012

In 2012 the UK-based HSBC Group was the subject of a USD 1.9 billion financial penalty, the imposition of a 'Compliance Monitor' and to intense media scrutiny and global condemnation, over lapses in its global anti-money laundering programme.

In July 2012 a report issued by the US Senate investigations subcommittee outlined five areas in which the bank had contravened US anti-money laundering, terrorist financing and sanctions laws. Specifically, between 2007 and 2009 more than 7 billion US dollars of suspect cash deposits from high-risk clients had been taken in by HSBC's Mexico operation. Between 2001 and 2007, the bank had stripped references to Iranian counterparties from 21,000 transactions worth 16 and a half billion dollars, involving potentially dangerous Iranians entities and furthermore the bank had provided US dollar banknotes to a bank called Al-Rajhi Bank, which had been founded by an Al-Qaeda benefactor who had provided services to Al-Qaeda affiliates. Between 2005 and 2008, it was found that HSBC in the United States had cleared 290 million dollars' worth of sequentially numbered travellers' cheques on behalf of Japanese bank Hokuriku Bank, which had, however, all been purchased from the same Russian bank. And finally, that the bank had provided accounts to thousands of companies which issued bearer shares – very high risk for money laundering since ownership of these companies, and hence the beneficiaries of any transactions which they conducted, would lie with whoever was in possession of the share certificates.

A couple of things are important to note here. First, the ferocity of the criticism levelled at HSBC didn't diminish because of the apparent absence of proven money laundering or terrorist financing. It was the fact that the bank was deemed to have been slack and haphazard in handling the risks,

which caused the damage to its reputation. The encouraging counterpoint, however, should be that if you are diligent in applying the necessary standards, and if the people who work in your bank do the things which they are meant to do, and if they achieve the standards which they are meant to achieve, then the actual presence of money laundering or terrorist financing activity within your organisation need not damage your reputation, because everyone accepts that AML and CFT isn't a zero sum game and cannot realistically be prevented completely.

Second, the financial cost to HSBC didn't stop with the fine. The remediation exercises that had to take place under the auspices of the monitor (in reality not an individual but a dedicated team from the consulting firm, Exiger), the payment of the monitor's costs, the remedying of other shortfalls identified during the monitoring period and the withdrawal from otherwise profitable businesses, cost it many hundreds of millions more in the years that followed (https://www.ft.com/content/0e3f0760-1bef-11e4-9666-00144feabdc0 "HSBC wrestles with the soaring costs of compliance")

Example

Danske Bank 2018

In 2015 reports began to emerge from Estonia that a whistle-blower at the Danish bank, Danske Bank's, Talinn branch had uncovered evidence of falsification of documents and money laundering within that bank's 'Non-Resident Portfolio' (NRP) there. Subsequent internal investigations over several years culminated in the September 2018 report of Danish law firm

Bruun & Hjeijle which outlined the extent of the AML failings at Denmark's largest bank, which included:

- lacking knowledge of customers
- lacking identification of (ultimate) beneficial owners and 'controlling interests'
- the presence as customers of various intermediaries from high-risk countries such as Russia and the former Soviet republics, which were unregulated and represented unknown end-customers
- insufficient attention to customer activities
- lacking identification of the source and origin of funds used in transactions
- no screening of customers against lists of politically exposed persons
- no screening of incoming payments against sanctions or terror lists
- in general, no automatic screening of incoming payments
- lack of response to suspicious customers and transactions.

While at time of writing (2019) we are only in the comparatively early stages of establishing what happened, how and why, several features of the Danske case already mark it out as being remarkable. Many of the underlying accounts were small shell companies with one or two officers (often the same name for multiple companies) and tiny balance sheets, as revealed in UK Companies House filings.Yet they were seeing funds flows of hundreds of millions of dollars in value. (NB I recommend www.grahambarrow.com for some excellent granular analysis of this case.) The amounts of laundering involved are believed to be very large – upwards of USD 200 billion equivalent have been identified so far – the majority of which went on to be cleared through the US financial system via Danske's

US correspondents, thereby exposing Danske to potentially massive financial penalties in the billions of dollars range. It was also, perhaps because of its size, a rare example where a money laundering scandal has led directly to the fall of a top level executive – Danske's CEO, Thomas Borgen, resigned in September 2018 upon the publication of the Bruun & Hjeilje report which the bank itself had commissioned. Finally, another unusual aspect was the finding of collusion among the branch staff, with several prosecutions now underway for alleged bribery with some branch staff having allegedly accepted financial inducements in return for their cooperation in opening accounts within the NRP. That is not a normal feature in these types of bank cases.

Example

Deutsche Bank 2017

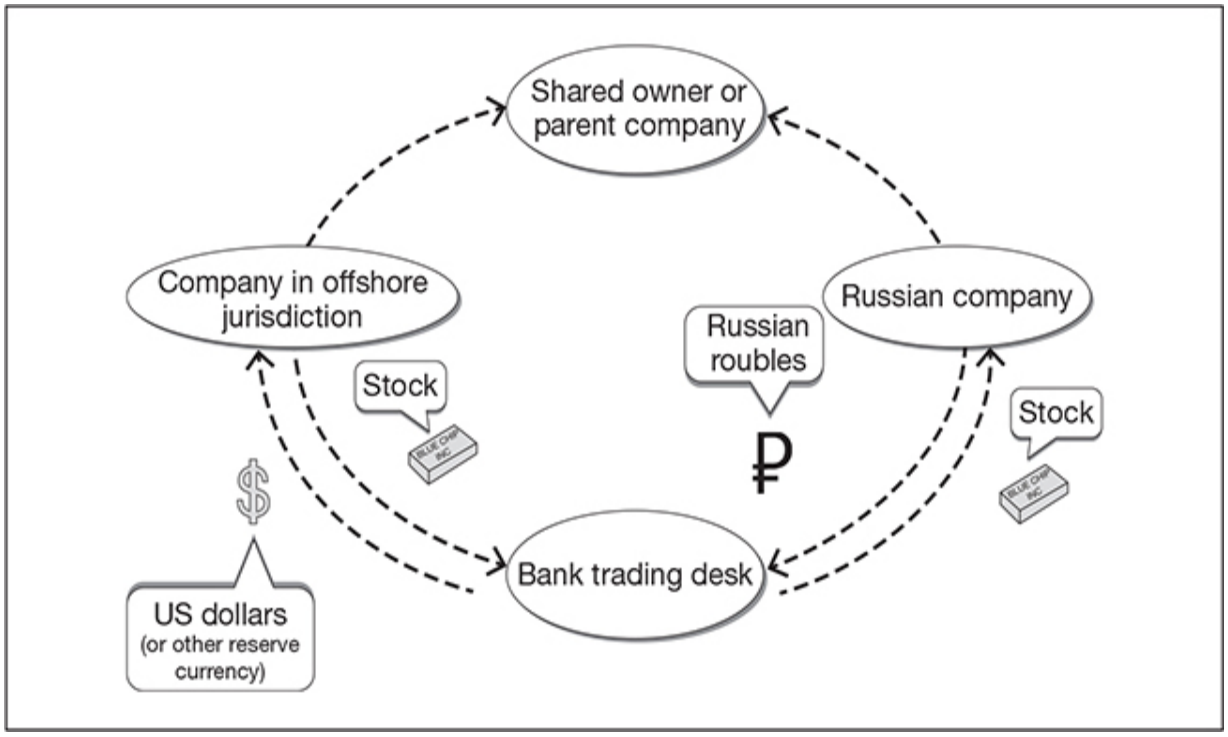
In 2017, Deutsche Bank agreed to pay a total of $630 million in penalties to US and UK financial authorities over accusations of having failed to have in place a proper culture, systems and controls to detect and prevent the movement of $10 billion equivalent out of Russia, through a trading scheme that bore the hallmarks of money laundering and which should have been detected.

Under the scheme, depicted in Figure 5.1, a broker for a Russian beneficial owner would speak to a Deutsche Bank sales trader and ask them to place two trades simultaneously. In one, he would use Russian roubles to buy a blue-chip Russian stock for a Russian company that his client owned. In the second trade, the broker – acting on behalf of a different company, which typically was registered in an offshore territory, such as the British Virgin

Islands – would sell the same Russian stock, in the same quantity, in London, in exchange for dollars, pounds, or euros. Both the Russian company and the offshore company had the same ultimate beneficial owner – the broker's client. Deutsche Bank was helping the client to buy and sell to himself.

The activity was not illegal in itself, but looked at in the whole (as opposed to on the basis of individual trades, which was how it seemed to be viewed within Deutsche Bank) it was an effective machine for removing billions of roubles from Russia, some of it possibly representing the proceeds of corruption, tax evasion and other crimes, as well as being in breach of exchange control and capital flight measures imposed by the Russian government.

Figure 5.1 **Mirror trading**



In its report, the UK's Financial Conduct Authority criticised the lack of effective AML systems and controls in detecting the transactions which, it said, were 'highly suggestive of financial crime'. The FCA also commented adversely on the cultural environment at Deutsche Bank, stating that

> ***'Deutsche Bank's culture failed to instil a sense of responsibility in the front office business for the identification and management of non-f inancial risks, particularly in the London Front Office, which failed to appreciate that it was ultimately responsible for Deutsche Bank's KYC obligations'***

Example

Australia Banking Corporation 2018

In August 2017 Australia's financial intelligence unit, the Australian Transaction Report and Analysis Centre (AUSTRAC) launched civil proceedings in the Federal Court of Australia alleging that CBA had breached money laundering and terrorism financing laws on 53,700 occasions. The breaches related to the bank's use of intelligent deposit machines (IDMs) between November 2012 and September 2015 – the bank claimed that a programming error allowed depositors to instantly credit cash deposits to their accounts, while failing to report amounts over $10,000 to AUSTRAC, and not enforcing any limits to the number of transactions. In February 2018, it was announced that CBA had reached a record-breaking settlement of the proceedings involving a payment of around AUD 700m (around USD 500m) – an Australian record. These financial crime proceedings came on the back of a number of other high-profile compliance and integrity related scandals which had afflicted the

bank in its financial planning, insurance and treasury divisions in recent years, and came amidst widespread industry rumours about the 'culture' at CBA. There has been frustrated and angry commentary in Australian public debate about the failure to hold very senior management in CBA to serious personal account.

Example

US Bancorp 2018

In February 2018, the US Justice Department announced that it had reached a $613 million settlement with US Bancorp over charges that the bank, through its subsidiary US Bank National Association, 'deliberately ran an inadequate anti-money-laundering program from 2009 to 2014. . . [and] failed to detect large numbers of suspicious transactions and concealed its missteps from regulators.'

The inclusion of the word 'deliberately' in the report is intriguing, but the reasons seem to have been different than the apparently deliberately corrupted programme run by the Estonian branch of Danske Bank, as outlined above. The finding of the Justice Department was that the US Bancorp subsidiary had set the parameters of their automated suspicious transaction reporting system at threshold levels which were geared towards staffing levels at the unit that would have to conduct the transaction analysis on the reports that were raised, rather than on properly assessed risk factors; in other words, that the tail of staff shortages was wagging the dog of money laundering and terrorist finance risk.

In a statement issued at the time of the announcement of the settlement, CEO Andy Cecere said: *'We regret and have accepted responsibility for the*

past deficiencies in our AML (anti-money-laundering) program. Our culture of ethics and integrity demands that we do better.' An intriguing aspect of the case was the lengths to which US Bancorp's Chief Compliance Officer (CCO) seems to have gone in order to conceal from the CEO the existence of known shortcomings in the AML programme (which were being pointed out to him on a regular basis by the head of financial crime compliance) – even to the point of deleting slides from within a PowerPoint presentation that was due to be made to the CEO, on the basis that they conveyed 'too negative' an impression. In this regard, this case (along with the Rabobank case referred to below) demonstrated the importance of having Compliance personnel at senior levels who, as was highlighted in the Introduction, are capable and prepared to 'speak truth to power' in ensuring not only that business which is unacceptable from an AML perspective is excluded, but also that the Compliance unit is provided with the necessary budget and resources to do its job effectively.

Example

Rabobank 2018

In February 2018, the California subsidiary of Dutch banking giant, Rabobank, pleaded guilty to obstructing investigations into its AML programme by its primary regulator, the Office of the Comptroller of Currency (OCC) and to deliberately concealing known deficiencies in the programme. According to the US Department of Justice, as required under the Bank Secrecy Act (BSA) Rabobank received regular alerts of transactions by 'High-Risk' customers, or through accounts deemed to be 'High-Risk,' and that had been the subject of prior SARs filed by

Rabobank. These High-Risk customers and accounts included those controlled and managed by Mexican businesses, non-resident aliens, and US-based accountholders who transacted hundreds of millions of dollars in untraceable cash, sourced from Mexico and elsewhere, into and through Rabobank accounts.

According to the DOJ, Rabobank created and implemented policies and procedures to prevent adequate investigations into these suspicious transactions, customers and accounts. Among those policies and procedures was Rabobank's 'Verified List' – under which Rabobank instructed its employees that if a customer was on the 'Verified List,' no further review of that customer's transactions was necessary – even if the transactions generated an internal alert, or if the customer's activity had changed dramatically from when it was 'verified.' Rabobank's BSA/AML staff were further instructed to aggressively increase the number of bank accounts on the Verified List, as evidenced by the fact that it had increased the number of 'verified' customers from just ten in 2009 to more than 1,000 in 2012.

Additionally, according to the DOJ Rabobank failed to monitor and conduct adequate investigations into these transactions and submit SARs to the Financial Crimes Enforcement Network (FinCEN), as required by the BSA. Rabobank's border branches, including those located in Calexico and Tecate in Imperial County, California, were heavily dependent on cash deposits from Mexico and Rabobank knew that millions of dollars in cash deposits at these branches were most likely tied to illicit conduct. In particular, the Calexico branch, located just a few hundred yards from the US–Mexico border, was the 'highest performing' branch in the Imperial Valley region due to the cash deposits from Mexico. Throughout the relevant time period, Rabobank continued its practice of soliciting cash-intensive customers from Mexico and elsewhere, all the while employing inadequate BSA/AML

policies and procedures to address the obvious high risks associated with these accounts.

According to the DOJ, during the OCC's periodic examination of Rabobank in 2012, Rabobank knowingly obstructed the examination, in particular by attempting to hide the outcome of third-party reports which detailed the ineffectiveness of the bank's BSA/AML programme.

Rabobank further demoted or terminated two RNA employees who were raising questions about the adequacy of Rabobank's BSA/AML programme.

An interesting feature of the case was the fact that one of the compliance executives who was heavily criticised and subject to a financial penalty and banned from acting as a compliance officer, Laura Akahoshi, was the former chief compliance officer at the OCC who had initially flagged up shortcomings in the Bank's BSA programme back in 2007.

Example

UBS 2007–2019

In February 2019, a French court fined the French arm of Swiss bank UBS €3.7 billion with a further €800m ordered to be paid in civil damages for assisting French clients of the bank evade French taxes. The verdict is the latest in a line of settlements and penalties against the bank (and others in the Swiss banking community, such as Credit Suisse) which can be traced to as far back as 2007, when UBS private banker Bradley Birkenstock turned whistle-blower to the US authorities on the assistance which the Bank was giving to wealthy American clients to avoid US taxes by placing undeclared wealth with it – an action which culminated in a USD 780

million penalty in 2009. Investigations also took place in a number of other countries, including Germany (€300 million penalty), Belgium, Israel and Argentina.

In 2011, the Paris public prosecutor's office opened a judicial investigation into UBS's laundering of tax fraud proceeds, suspecting it of implementing a 'double accountancy' system in order to mask the movement of capital between France and Switzerland. In 2013, UBS France, followed by UBS AG, was accused of soliciting wealthy French citizens at sports events and concerts and encouraging them to open undeclared bank accounts in Switzerland. Then, in 2014, UBS was indicted for aggravated laundering of the proceeds of tax fraud and bail was set for €1.1bn, which UBS contested to no avail in the European Court of Human Rights. The following year, three former UBS directors in charge of wealth in western Europe and France were issued with a French arrest warrant while Raoul Weil, the former chief executive of UBS wealth management, was placed under investigation. And in February 2019, French judges ordered UBS to pay a record € 3.7 billion fine for carrying out what prosecutors said was a long-running scheme to help French clients hide huge sums of money from the authorities. (UBS is appealing the verdict.)

Example

ING Bank 2018

In September 2018, the Dutch bank ING Bank N.V. accepted and paid a settlement of €775,000,000 offered by the Netherlands Public Prosecution Service (NPPS), which had accused ING of violating the Netherlands Anti-Money Laundering and Counter Terrorism Financing Act for many years *on*

a structural basis (author's own italics). It is worth noting that the events described below followed years of warnings issued to ING by the Dutch Central Bank, which it had apparently failed to act upon.

The investigation by the Dutch authorities started at the beginning of 2016, following several criminal investigations in which it was noticed that the parties being investigated held accounts with ING, leading to suspicions that ING was not sufficiently investigating clients, was insufficiently monitoring bank accounts and either did not report unusual transactions, or reported them much later than was required by the law.

The NPPS provided details of some of the incidents of money laundering which had been investigated, which included:

- an international telecom provider which transferred bribes worth tens of millions of dollars via its bank accounts with ING to a company which was owned by the daughter of the then president of Uzbekistan
- a women's underwear trader which was able to launder approximately €150,000,000 through its bank accounts held with ING
- a Suriname-based one-man business in building materials, with no address in the Netherlands, to which 15 mobile ATMs were linked and to which nearly €9 million was transferred, even though no building materials were purchased for that amount – in reality, debit cards were used in the mobile ATMs in Suriname in exchange for cash
- in less than a year, more than EUR 500,000 was deposited in cash into the ING bank accounts of two connected companies, apparently for the purpose of importing and trading in fruit and vegetables from South America, but in reality probably a front for money laundering.

The failure count bears sadly predictable similarities to many other cases, including the Danske Bank case referred to earlier and which included:

- poor or non-existent client due diligence
- acceptance of clients without sufficiently investigating the risks associated with those clients
- clients being classified in the wrong client segments
- insufficient monitoring of client relationships and bank accounts
- failure to terminate client relationships in a timely manner, where the risks didn't justify continuation
- the compliance department was understaffed and inadequately trained
- due to budget constraints, the transaction monitoring system only generated a limited number of money laundering alerts, such that *'only the proverbial tip of the iceberg was investigated'*
- if an unusual transaction was nevertheless recognised, it was regularly *not* reported to the FIU, or was reported too late.

However, despite the bank effectively having been found to be systematically, institutionally culpable for money laundering, as noted in the Introduction, this culpability did not extend to senior individuals, who were effectively exonerated from criminal guilt by virtue of their ignorance of what had been going on.

Example

ABN AMRO 2004

ABN AMRO fell foul of the US AML regulatory system, which required that banks must have a programme 'reasonably designed to assure and monitor compliance' with AML laws. ABN's North American clearing centre in New York dealt with 30,000 fund transfers a day and had clients that were deemed to be high risk including hundreds of shell banks (a shell bank, it may be recalled, is a 'virtual' bank with no physical presence in its country of incorporation and which is not part of a larger banking group). Upon inspection, FINCEN (the US's Financial Intelligence Unit) found that violations of the Bank Secrecy Act 'were serious, long standing and systemic'. Only one person was in charge of monitoring this activity. There had been sporadic manual monitoring to start with and when suspicious activity reporting was automated, many reports were produced which, however, were never acted upon. There was inadequate due diligence on bank customers from higher-risk jurisdictions or in connection with higher-risk transactions, despite the fact that there had been numerous regulatory warnings about such customers and transactions. A poor record of suspicious transaction reporting, a non-existent training programme and no proper system of internal controls compounded the problems. ABN was fined $30 million along with other fines.

Example

Lloyds Bank 2009

In 2009 the UK-based bank, Lloyds TSB, was fined in the US after admitting to falsifying information on hundreds of millions of dollars' worth of international wire transfers – the electronic messages through which payments are made between counterparties in different countries.

The wire transfers in question involved companies in countries that were the subject of sanctions by the US government. US investigators were probing links between the Iranian government and two Manhattan-based companies when they stumbled on a trail of Iranian money entering the city via Lloyds. The UK branch of an Iranian bank would send an electronic payment message to Lloyds via the SWIFT system. However, knowing that the suspicion of the US authorities would be alerted if the payment message made reference to Iran or to an Iranian company as the source of the funds, Lloyds staff would then re-key the data in the SWIFT message, leaving out any reference to Iran, before sending it on to the US. This process was known as ‘stripping’. It didn’t come about through the misdemeanours of a few rogue staff. Rather, it happened under standing operating instructions.

The US authorities have electronic filters to detect wire transfers from sanctioned countries, but the lack of identification details meant that the Lloyds transfers could get through, especially since they came from a reputable UK bank. Taken with other transactions involving another sanctioned country, Sudan, when confronted by the US authorities Lloyds admitted to over $350 million of illegal transactions between 2001 and 2004. The transfers in question were made to buy goods and services from US companies and from companies in other countries that wanted payment in dollars. The Manhattan District Attorney’s Office said that they feared that some of the funds ‘may have been used to purchase raw materials for long-range missiles’. Lloyds was hit with a fine of $350 million – at the time the biggest penalty ever against a single financial institution for breaches of sanctions legislation. The bank also had to conduct an audit of a wide range of other transactions over the period in question to determine their legitimacy.

Two historical case studies

It's important not to allow the lessons of the past to be lost in the rush for yet more and more up-to-date information. So I have included here two historical cases for the enduring light which they shine on the ways in which things go wrong. The shortfalls identified in these cases are disappointingly easy to recognise in the modern cases examined above.

Example

Citibank – Salinas 1999

A PEP comes calling

Raul Salinas was the brother of the former President of Mexico, Carlos - Salinas. For five years during the late 1980s he was Director of Planning for Conasupo, a Mexican state-run agency regulating certain agricultural - markets, with an annual salary of up to $190,000. From 1990 until mid-1992, he was a consultant at a government anti-poverty agency called Sedesol.

In January 1992, Carlos Hank Rohn, a prominent Mexican businessman and long-time client of Citibank's private bank, telephoned his private banker, Amy Elliott, and asked her to meet with him and Raul Salinas that same day. Elliott was Citi's most senior private banker in New York handling Mexican clients. At the meeting in New York, which was also attended by an even more senior private banker, Reynaldo Figueiredo, Carlos Hank provided the bankers with a strong personal reference for allowing Salinas to open an account. In May 1992, Elliott flew to Mexico and duly obtained Salinas' signature on account opening documentation. She proposed accepting him as a client without investigating his employment background, financial background or assets, and waiving all references other than the

one provided by Mr Hank. The head of the Western hemisphere division of the private bank, Edward Montero, approved the opening of the account. Such was the secrecy involved that the private bank's country head in Mexico, Albert Misan, was not consulted and apparently did not even learn of the existence of the account until 1993. In June 1992 Elliott wrote in a monthly business report that the Salinas accounts had *'potential in the $15 to 20 million range'*.

Account set-up

After accepting him as a client the private bank opened multiple accounts for Mr Salinas and his family. The New York office opened five accounts and the private bank's trust company in Switzerland talked to him about opening additional accounts in the name of a shell corporation (a nameplate company existing as a purely legal entity, not as an operational one). A Confidas employee wrote in June 1992:

> **'The client requires a high level of confidentiality in view of his family's political background . . . This relationship will be operated along the lines of Amy's 'other' relationship; i.e., she will only be aware of the 'confidential accounts' and will not even be aware of the names of the underlying companies . . . Please note for the record that the client is extremely sensitive about the use of his name and does not want it circulated within the bank. In view of this client's background, I think we will need a detailed reference from Amy, with Rukavina's [Hubertus Rukavina – the head of the private bank and a Confidas board director] sign-off for our files . . . '**

The ‘detailed reference’ was never obtained and neither was Rukavina’s sign-off, yet Citibank in the Cayman Islands activated a Cayman Islands shell corporation called Trocca Ltd to serve as the owner of record for private bank accounts benefiting Mr Salinas and his family. Cititrust used three additional shell or ‘nominee’ companies to function as Trocca’s board of directors, Madeline Investments SA, Donat Investments SA and Hitchcock Investments SA, and a further three nominee companies to serve as Trocca’s officers and principal shareholders, Brennan Ltd, Buchanan Ltd and Tyler Ltd. Cititrust controlled all six companies which were routinely used to serve as directors and officers of shell companies owned by private bank clients. Approximately one year later Cititrust also established a trust, identified only by a number (PT-5242), to serve as the owner of Trocca. The result of this elaborate structure was that Mr Salinas’ name did not appear anywhere on Trocca’s incorporation papers. Separate documentation establishing his ownership of Trocca was maintained by Cititrust in the Cayman Islands, under secrecy laws restricting its disclosure. Even Amy Elliott was not aware of the name of the shell corporation and Mr Salinas was not referred to by name, but by the acronym ‘CC-2’, or ‘Confidential Client No. 2 (CC-1 being Carlos Hank Rohn).

After Trocca was established the private bank opened investment accounts in London and Switzerland in the name of Trocca and later, in 1994, a special name account was opened for Mr Salinas and his wife in Switzerland under the name of ‘Bonaparte’.

Movement of funds

After his accounts were first opened, Mr Salinas made an initial deposit of $2 million via the account of Carlos Hank, who told the bank that these were monies provided by Salinas in respect of a business transaction which never proceeded. The funds were divided between the Salinas accounts in

New York and the Trocca accounts in London and Switzerland. But it was in May 1993 that the arrangements under which the bulk of the Salinas funds were to be moved were set up. Elliott met with Salinas and his mistress (later to become his fiancée), Paulina Castaˇnon, at his home in Mexico, where he explained that he wished to move funds out of Mexico to avoid the volatility which traditionally accompanied Mexican elections. In order to provide maximum confidentiality on this undertaking, it was also agreed that Ms Castaˇnon, using an alias 'Patricia Rios' (Rios being her middle name) would deposit cashiers' cheques with Citibank's Mexico City branch, from where the funds would be wired through to a Citibank account in New York, for onward transmission to the London and Switzerland accounts. Although senior management in Mexico denied knowledge of the arrangements, Elliott herself cooperated fully, even setting up a meeting between herself, Castaˇnon/Rios and a service officer at the Mexico City branch to explain the arrangements and ensure that the cheques would be accepted.

Cashiers' cheques were a form of instrument, similar to a bank draft, which were drawn on the banks themselves and which did not, therefore, reveal the beneficial owner of the funds in question, and the New York account to which the funds were then to be wired (marked for Amy Elliott's attention) was a 'concentration account' – an account which commingled the funds of various clients with other funds belonging to Citibank itself, without revealing who owned what. Given that neither Salinas nor Castaˇnon/Rios held any accounts with Citibank in Mexico City (which must therefore have received the funds into its own nostro accounts), and given that the Salinas accounts in London and Switzerland were trust company or code name accounts, these arrangements had the effect of disguising completely the

beneficial ownership of whatever volume of funds would eventually pass through them (see Figure 5.2) .

Source: http://www.gao.gov/archive/1999/os99001.pdf

These funds turned out to be substantial, and in any event way above the initial '$15–20 million range', referred to by Elliott in her June 1992 business report. The sums involved were very large and were deposited within very short periods. For example, in May and June 1993, in a period of less than three weeks, seven cashiers' cheques were presented to the Mexico City branch totalling $40 million, and over a two-week period in January 1994 four cashiers' cheques totalling $19 million were deposited. By the end of June 1994 the total funds in the Salinas accounts originating from Mexican cashiers' cheques amounted to $67 million.
A further $20 million was transferred using other methods, leading to a grand total in excess of $87 million. In June 1993, Elliott emailed a colleague in Switzerland:

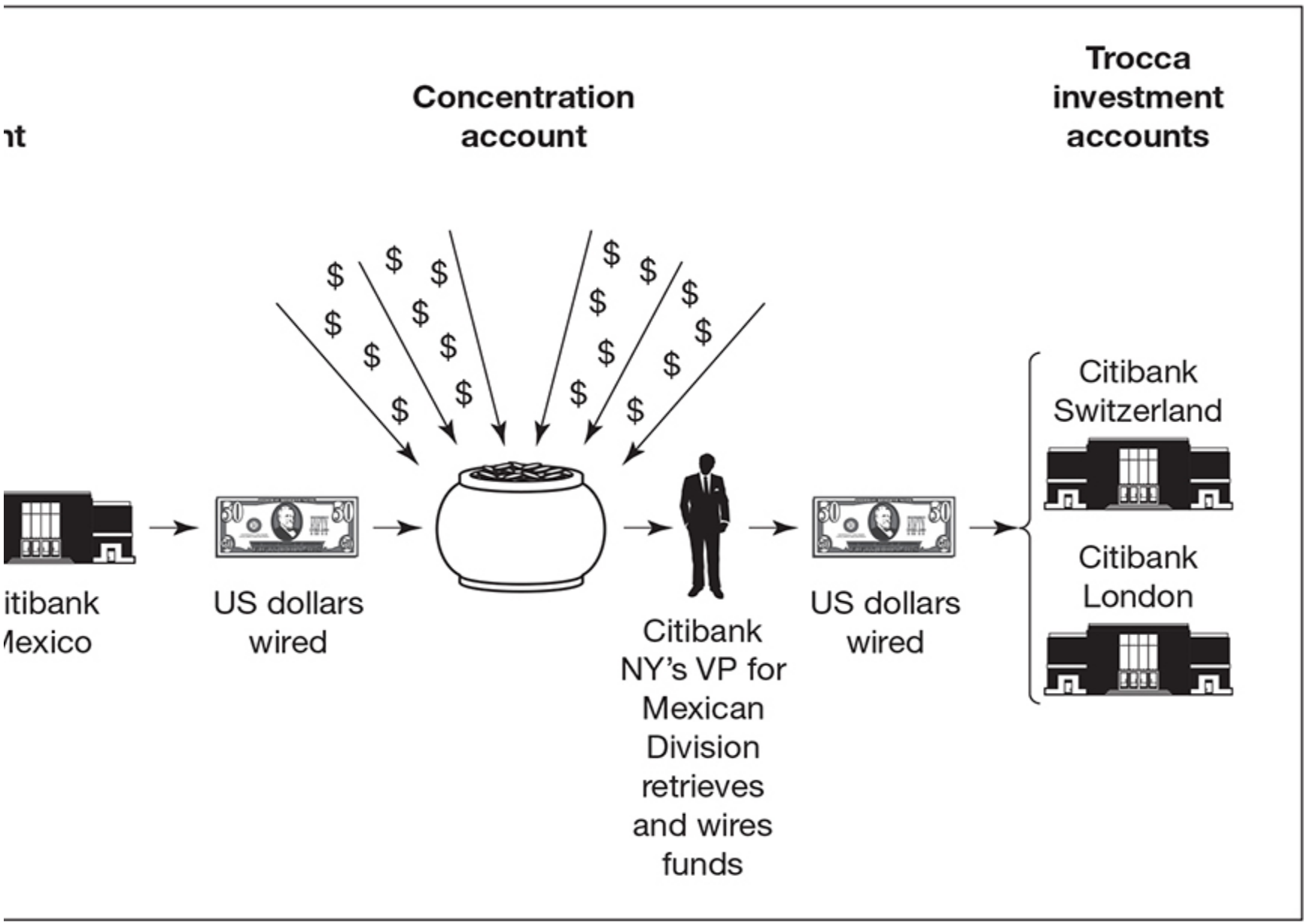
> **'This account is turning into an exciting and profitable one for us all. Many thanks for making me look good!'**

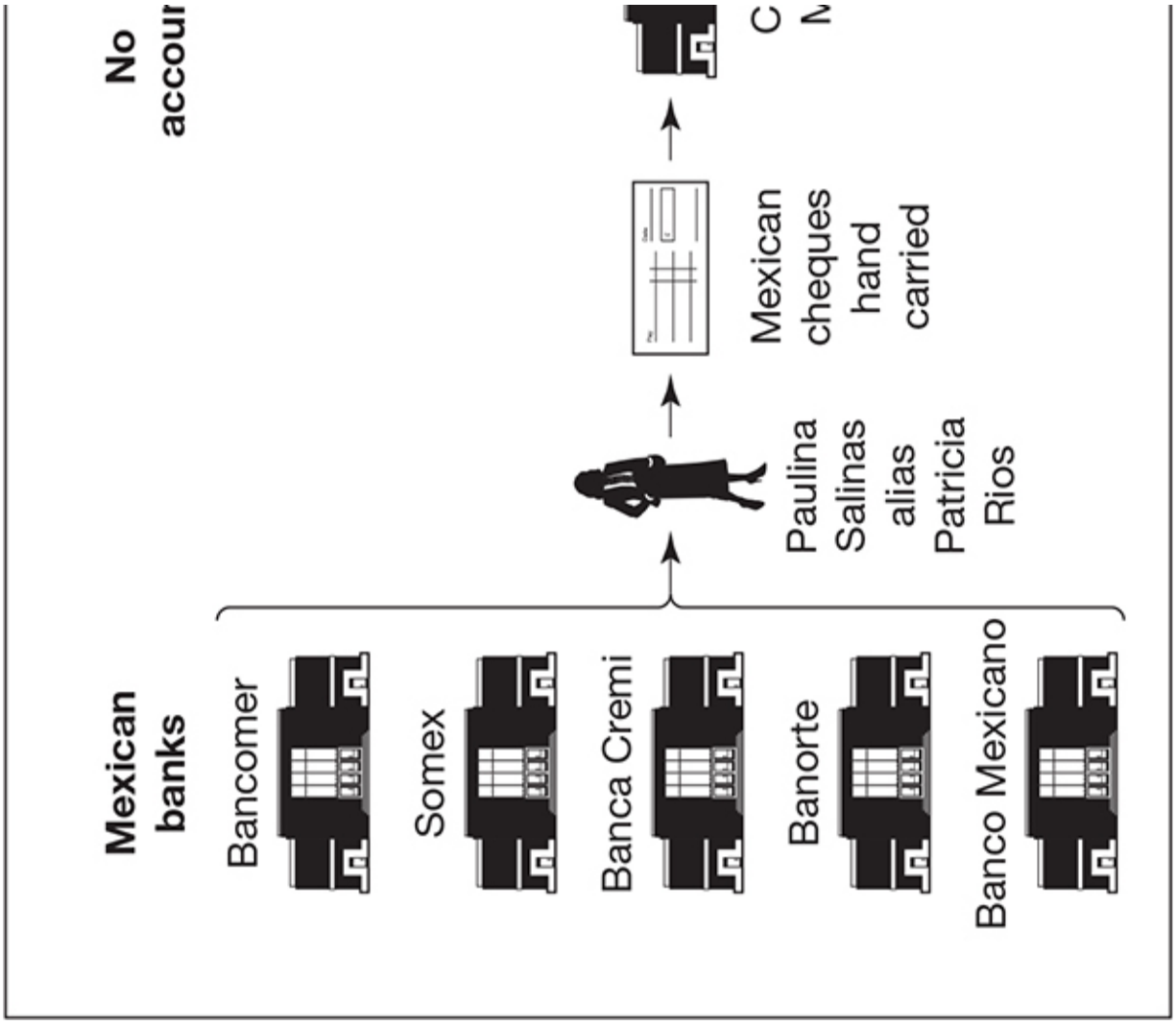
The Salinas arrests and the private bank's reaction to them
In early February 1995, the Mexican press started to report that Salinas was under suspicion of murdering his former brother-in-law, Luis Massieu, a leading Mexican politician. Questioned by a presumably concerned Elliott, Salinas claimed that the charges were politically motivated and untrue. Then, on 28 February 1995, he was arrested and imprisoned in Mexico on suspicion of murder. (After a lengthy trial, a conviction followed, which was upheld on appeal in 1999.) Nine months later, on 15 November 1995, Salinas' wife was arrested in Switzerland and the following day the Swiss

authorities froze more than $130 million sitting in Salinas controlled accounts with various banks – including Citibank. The rumours were that the Swiss authorities were investigating allegations that Salinas had been involved in laundering the proceeds of illegal narcotics and, sure enough, three years later in October 1998, proceedings in Switzerland were commenced on that basis.

The private bank's reactions to this reputational disaster unfolding before it have since become well documented, as has Amy Elliott's role as the classic relationship manager 'caught in the middle' of a corporate environment that claimed that anti-money laundering (AML) and client due diligence (CDD) policies were important, but which also, at that time, apparently did not enforce them consistently enough. They are revealed in detail within the pages of the report on the hearings of the Senate Committee on Investigations on private banking and money laundering in November 1999, and show the following.

Figure 5.2 **Citibank – Salinas flow of funds**


nt
Concentration account
Trocca investment accounts
itibank Mexico
US dollars wired
Citibank NY's VP for Mexican Division retrieves and wires funds
US dollars wired
Citibank Switzerland
Citibank London



■ *Initial reactions*: in March 1995, soon after Salinas had been arrested for murder, tape transcripts of conversations between the bank's New York, London and Swiss offices reveal that the initial instincts of the bankers, far from making life easier for the law enforcement investigations which were bound to follow, were rather to make it in practice more difficult for them. For example, the then head of the private bank, Hubertas Rukavina, mooted sending the funds held in the London accounts over to Switzerland so as to make their discovery more difficult – an option which was considered but rejected, apparently, however, primarily on the grounds that the

transfer would be obvious in London's books. The same transcripts also reveal that the bankers discussed calling in loans which had been made to Trocca against its deposits, so as to ensure that the bank was not out of pocket in the event that the Trocca funds were frozen.

- *Absence of due diligence records*: it became clear during the hearings that despite the existence of clear policies requiring that information on clients' backgrounds and sources of wealth be collected within the bank's CAMS (Client Account Management System), in fact no entries had been made at all regarding Salinas. There had been a complete blank throughout the three-year period of the relationship.
- *Backdating of due diligence records*: it then became clear that what records there were had only been completed *ex post facto* by Elliott in early March 1995 following Salinas' arrest, apparently at the behest of private bank senior management in London who wanted to feel 'more comfortable' about the source of wealth on the account, upon which in fact there was very little knowledge. Furthermore, faced in November 1995 with a request for information from the Swiss authorities following the arrest of Salinas' wife in Switzerland, the bank's legal department (who by now had operational control of the accounts) had effected further, after-the-event changes to the CAMS entries. They incorporated reference to a belief that Salinas had sold a construction

company – something which Elliott had not included in her own initial attempts at completing the CAMS profile back in March 1995. None of the information had been verified to the extent required by bank policy.

■ *Absence of effective enforcement of due diligence policies*: the senate hearings record how: 'during this same period, 1992 until 1995, top leadership in the Western Hemisphere division had sent numerous strongly worded memoranda urging, and ultimately ordering, its private bankers to complete and update information on their client account profiles' and how 'Several internal audits had specifically identified incomplete client profiles as a problem.'

Yet apparently nothing effective had been done to ensure that these instructions were followed. None of the senior managers who waived additional personal references for Salinas beyond the Hank reference, enquired as to what other background checks were being made on - Salinas and Elliott herself clearly believed that senior management – right up to the very top of the organisation – was both aware of and approved of the Salinas accounts, regardless of whether or not due diligence information was available. The account had earned $2 million in fees and interest for the bank and tapes of conversations made on the day after Salinas' arrest recorded Elliott saying: 'Everybody was on board on this . . . I mean this goes in the very, very top of the corporation, this was known, okay? . . . We are little pawns in this whole thing, okay?'

■ *Restricted reporting to the authorities*: the exact reporting obligations of any bank in the situation in which Citibank found itself, in terms of timing and content, will always be a matter of a legal interpretation dependent on a number of factors. But the senate

documents make the point that when the bank filed a criminal referral form with US law enforcement officials on 17 November 1995 – the day after the freezing of the Swiss accounts – the report only referred to the New York accounts, which held only $200,000, and not to the London or Swiss accounts which held over $50 million.

- *Failure to identify discrepancies between actual and expected account activity*: Elliott had stated in her earliest business report that the account had potential in the '$15–20 million range', yet when the funds actually passing through the Salinas accounts topped $87 million – more than four times what was apparently expected – this did not trigger alarm bells or generate any action to validate the source of this apparently unanticipated stream of wealth.

The case concludes

Having started with a bang, the Salinas case concluded more quietly. The US District Attorney's Office initiated an investigation into whether money laundering charges should be filed against Citibank or any of its employees, but decided against it – presumably because there was no evidence that anyone in Citibank had suspected wrongdoing and therefore participated willingly in any scheme. It is always difficult being judged by new standards and it is possible to argue that, as the banking industry emerged from the world of 'anything goes' into the new era of regulation and public scrutiny, that this was the position which Citibank effectively found itself in. Its Chief Executive, John Reed, who apart from his appearance before the Senate Committee was also forced to endure the indignity of a day in the company of the Justice Department being interviewed about the affair, wrote to the Citibank board:

> **'Much of our practice that used to make good sense is now a liability. We live in a world where we have to worry about 'how someone made his/her money', which did not used to be an issue. Much that we had done to keep private banking private becomes 'wrong' in the current environment . . . '**

Amy Elliott, too, in some ways found herself betwixt two worlds, and paid a very public price for it. After describing the positive perceptions of the Salinas family which she had built up over the years, and the habits of Latin American elites in moving sometimes vast sums overseas in order to escape market volatility caused by political turmoil, she stated in her written testimony before the Committee:

> **'It is easy to ignore the context I have described and instead to focus on isolated details in this matter and make them seem questionable. The world in which I operated as a relationship manager in the early 1990s was different from the private banking environment today. Procedures, technologies and safeguards are very different today at Citibank . . . I only ask you, with all due respect, to keep in mind the broader picture I have described as you frame your enquiry to me.'**

Source: http://www.gao.gov/archive/1999/os9900/.pdf

Lessons learned

The world was surely different back then, and if you're a financial crime professional, re-reading the case makes you realise just how far things have come since the early to mid-nineties; Wolfsberg, the Patriot Act, EU III, IV and V the risk-based approach have all come into being. And yet despite the passage of time, some of the issues this case raises are timeless.

- If you have a state-of-the-art compliance policy, what good is it if it isn't followed at the 'coal face'?
- If mixed messages are being sent out with firm AML policies on the one hand but a failure to deal with non-compliance on the other, where does that leave the relationship managers – the 'poor bloody infantry' who have to deliver both compliance and revenue?
- If the corporate culture is perceived by staff as prizing revenue above all else, then where does that leave the organisation as a whole in terms of its reputational exposure when things go wrong?

Shortfalls identified included:

- no proper identification of the customer
- no effective KYC on the customer relationship
- adequate documentary links between client identity and ownership of assets were not maintained
- information on sources of wealth were not obtained
- the substantial discrepancy between expected versus actual funds - volume was not spotted . . .
- and as a result, suspicious activity was not reported
- there was a delay in making a suspicious activity report for six months
- account documentation was doctored after the event to make it look as if proper KYC had been done
- staff were not supervised properly to ensure the KYC policy was being implemented
- senior management ignored multiple audit warnings.

Example

Riggs Bank – Augusto Pinochet 2002

Riggs Bank was a Washington DC-based prestige bank which had built up its reputation over 150 years. It had served 20 US presidents including Abraham Lincoln and had supplied gold for the Alaska purchase in 1867. A major line of business for Riggs was the operation of accounts for foreign embassies in the US capital. Often this extended into private banking for diplomats, their family members and sometimes other officials from the country in question.

Under the US Bank Secrecy Act, banks at that time, and indeed now, were required to maintain an extensive compliance programme which included requirements that they perform due diligence against their customers, that they identified suspicious transactions involving funds of potentially illegal origin and that they report suspicious transactions to the authorities. Riggs' own Bank Secrecy Act compliance programme policies and procedures stated that:

> **'Riggs Bank will conduct business only with individuals, companies, trusts (beneficial owners) and grantors/power holders of such trusts that we know to be of good reputation and, through proper and thorough due diligence, we know to have accumulated their wealth through legitimate and honorable means.'**

Augusto Pinochet Ugarte was a boy from a middle-class Chilean background who rose to become a general in the Chilean army and who seized power from the elected president Salvadore Allende in a bloody coup in 1972. Several years of violent repression followed with some reports putting the number of deaths under Pinochet's regime as high as 3,200, with

tens of thousands imprisoned and tortured. During his rule, until his resignation in 1989, he was also accused of having connections with drug trafficking and illegal arms sales, and of corruptly accruing $28 million. But Pinochet still wasn't a 'bad guy' that everyone could agree on. Millions of Chileans and many in the West supported him because they believed he had saved the country from Communism and directed it firmly and safely to the path of economic growth and prosperity.

It was against this background that in 1994 a senior delegation of Riggs Bank executives visited Chile to solicit General Pinochet's business. His first personal account with Riggs was opened shortly thereafter, an account which saw balances ranging up to $1.2 million over the next few years. The Riggs Bank approach came despite the fact that General Pinochet was already known internationally as a controversial figure and despite this, in all that followed, no evidence was ever found of any KYC documentation on his account created or maintained by Riggs Bank. Some 18 months after the account was opened, Pinochet was indicted in Spain for crimes against humanity.

Between 1994 and 2002 Riggs opened three more personal accounts for Pinochet, these being a money market account which held balances up to $550,000, a checking account and a 'NOW' account, which contained balances of up to $1.1 million. Riggs also established corporate accounts with complex structures for the Chilean ex-president. These included offshore shell corporations (i.e. corporations with no real physical presence, employees or staff) for the receipt of certificates of deposit which benefited General Pinochet and his family. The companies, Ashburton Limited and Althorp Investment Co Limited, all had nominee shareholders (a function which was performed by Riggs Bank (Bahamas) and directors and officers from the accounting firm which was managing the affairs of Riggs Bank in

the Bahamas). So Pinochet's name didn't appear anywhere on the incorporation papers. At times, these corporate accounts held balances up to $4.5 million.

Much of this activity was occurring despite the fact that in 1998 the Spanish courts had issued international warrants for General Pinochet's arrest and had issued attachment orders against his accounts throughout the world. In the UK, Pinochet had been arrested pursuant to the Spanish warrant and was subject to an extradition hearing. Yet no suspicious activity reports were filed by Riggs, which continued to operate the Pinochet accounts without the knowledge of the US authorities. In May 2001, a senior executive at Riggs, Stephen Pfeiffer, forwarded a memo to two senior Riggs Bank officials, containing extensive information on Pinochet's alleged crimes and the litigation surrounding him.

In the spring of 2002, during a routine examination, the Office of the Comptroller of the Currency (OCC) discovered evidence of the Pinochet accounts at Riggs. Initially the Bank resisted cooperating with the investigation, but in the end it did cooperate and finally, in the summer of 2002, the Pinochet accounts were closed. Federal regulators fined and required various contributions from Riggs Bank to a total sum of $53 million and World-Check has estimated that $130 million was wiped from Riggs' share value as a result of this and other money laundering scandals. In July 2004 Riggs Bank was sold to the PNC Financial Services Group Inc. and the famous 150-year-old name became extinct.

In its reports on the Pinochet accounts and other accounts where Riggs Bank fell short, the US Senate Permanent Sub-Committee on Investigations stated that 'Riggs has disregarded its Anti-Money Laundering (AML) obligations, maintained a dysfunctional AML program despite frequent

warnings from OCC regulators, and allowed or, at times, actively facilitated suspicious financial activity.'

Lessons learned

How should we assess the significance of the Riggs Bank/Pinochet case and what lessons can be learned from it? Clearly it was very significant because it was one of a number of cases which pointed out the very real reputational risks that exist in doing business with controversial political figures. A key lesson learned from the case is the importance of undertaking a comprehensive risk assessment before a relationship has commenced, which covers not just the sources of wealth and the origin of the funds expected to come into the account, but also the wider reputational issues surrounding allegations against the potential client – both current and historic. If Riggs Bank *did* do this, then clearly they got it badly wrong. Secondly, it is important that with such individuals, such assessments – and the due diligence which goes with them – should not be a 'one-off' event, but should take place on a constant and regular basis, such that new evidence concerning the client is taken into account and processed and so that there can be an ongoing assessment about the suitability of a particular client for a continued business relationship. In this regard, the Riggs Bank/Pinochet case also demonstrates the importance of not allowing relationship managers who may have developed a very close personal relationship with a client, or who may be influenced by their own political views, to override the organisation's wider sensors regarding the continued suitability of a particular account. Finally, failures in suspicion reporting and in the level of KYC and due diligence on an account will always be punished heavily by regulators, and this case was no exception.

Source: Based on facts from
www.access.gpo.gov/congress/senate/pdf/109hrg/20278.pdf

MANAGING REPUTATIONAL RISK: THE EXPERIENCE OF THE MDBS

Forging a workable policy for managing reputational risk

Multilateral Development Banks (MDBs) and International Financial Institutions (IFIs) have devoted a lot of attention in recent years to developing their management of reputational risk. They face a difficult task. On the one hand, they are mandated to invest and lend in countries which badly need them, such as less developed economies in the former Communist world, parts of Asia, Africa, the Middle East and Latin America. After all, there is no point in such institutions existing if they are not going to make funds available to help improve people's lives. On the other hand, the very places where the funds are most needed are, almost by definition, high risk. They often have high levels of corruption and crime. Their institutions are either new and less rooted than their equivalents in the developed world or have actually been compromised by corruption and crime for many years. 'Integrity' and 'transparency' are viewed by many as luxuries in societies where the only way to get on has been to play fast and loose with whatever rules exist and to get as far as you can as quickly as you can, making whatever accommodations are necessary with the authorities.

How, then, should such institutions deal with applications for financing from, say, a private sector entrepreneur whose business plan seems to offer good returns and great benefits (potentially) to the economic development of the country, but whose past is often shrouded in mystery? This is a crucial question when the past activities of the people concerned may come back and bite the ankles of the institution in a very public way. Just as importantly, regardless of the negative publicity, if they lend to or invest in

‘the wrong person’ then the project itself is unlikely to be successful. Are the MDBs then part of the solution or part of the problem?

Integrity due diligence

Commercial banks may not possess the same social and economic development obligations of the MDBs and IFIs. But particularly since the 2008 financial crisis, the social impact of their operations has never been under such close scrutiny. You can argue about the value or otherwise of allegedly ‘socially useless’ proprietary trading and arbitrage activities, but the provision of financial services to wicked despots and dodgy business people and politicians is universally unpopular and today’s banks need some kind of framework within which to analyse a range of integrity-related reputational risks. These risks extend beyond money laundering and terrorist financing into corruption, tax evasion and other forms of criminality, political exposure, corporate governance, regulatory investigations and lawsuits, and the general personal and corporate reputations of the people and companies involved.

The advantages of having such a framework are clear. While each case is unique and must be looked at on its merits, passing each through a common framework of assessment and analysis introduces consistency into what might otherwise be a very subjective process. It forces people to ask difficult questions and provides a common way of both finding the answers and assessing the impact of the answers, all looked at through the prism of the organisation’s reputation: ‘doing the right thing’ and (just as important) being seen to be doing the right thing.

In order to gain some perspective on this, we will look now at the type of framework being followed increasingly by a number of the MDBs/IFIs. What is described here is a generalised version of what are in fact a number of different processes which are specific to each institution. Nevertheless the broad principles tend to be the same.

The process is known as the Integrity Due Diligence (IDD) process. Its key components are:

- an integrity red flags checklist – a list of questions designed to elicit
- relevant information (see Table 5.1)

- due diligence research tools – ways of obtaining that information (see Table 5.2)
- IDD assessment guidelines – policy guidance on interpreting the information and making decisions.

In essence the process is as follows.

The IDD process: initial stage

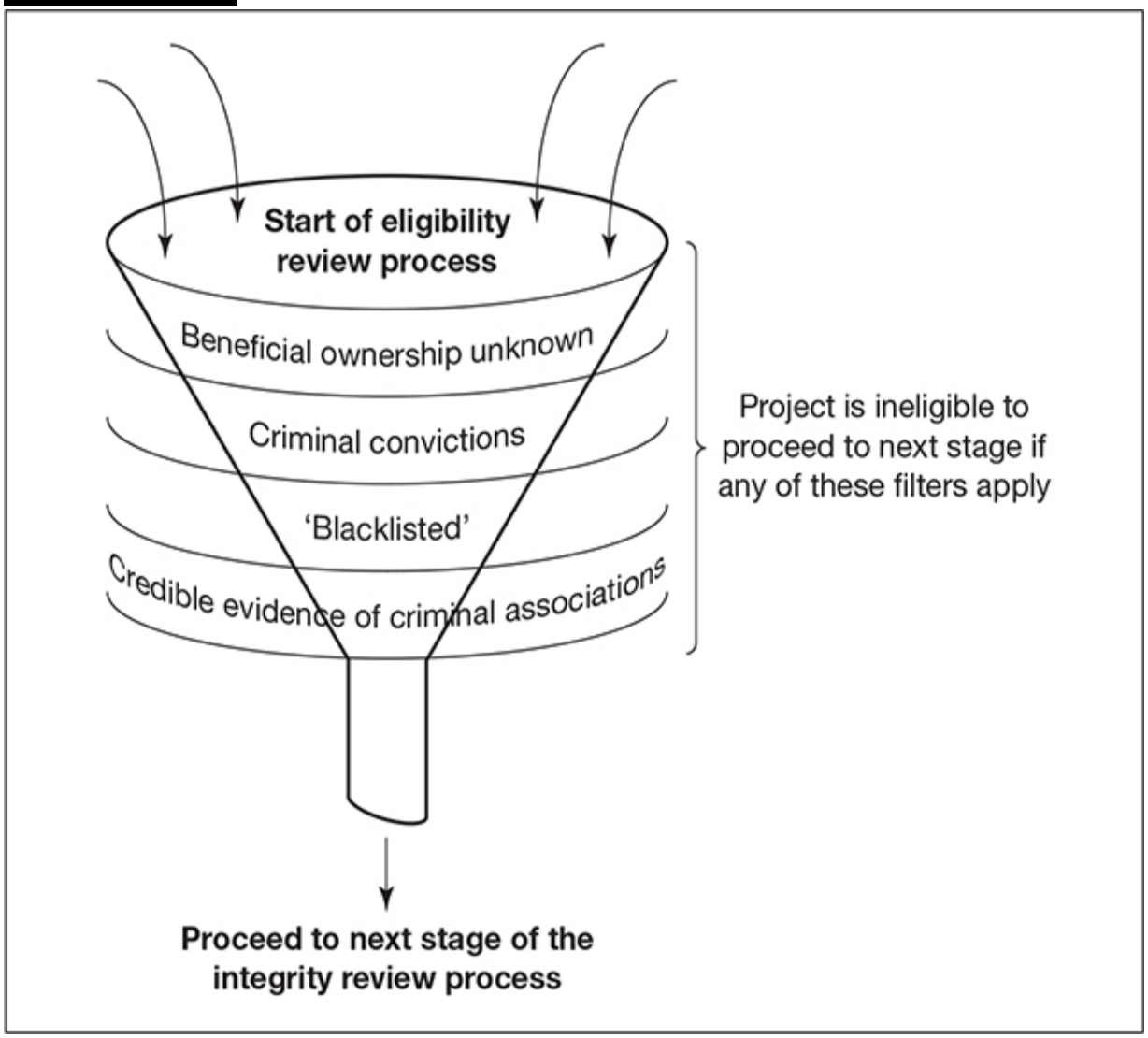
After the project has been proposed in concept form (usually as a result of a proposal by an applicant), a detailed investigation is undertaken by the banking team responsible for the transaction using the red flags checklist and the due diligence research tools. Documents and other evidence are filed and the outcome of the investigation is subject to an initial, conceptual 'in principle' assessment, using the IDD assessment guidelines, to determine whether it passes a 'funnel test' of policy principles. This stage of the process is depicted in Figure 5.3.
The four filters shown in Figure 5.3 are drawn from the IDD assessment guidelines and stipulate the circumstances which, all else being equal, will effectively prevent the deal from going any further. They are embodied in the following principles:

1. The transaction cannot proceed if beneficial ownership is unclear

This is a base-level requirement – if you don't know who the ultimate beneficial owner of a business, structure or asset is, then how can you be sure that it is not owned by a criminal, a terrorist or a political figure? Corporate structures must be investigated back up the chain until all significant beneficial owners have been identified. If this cannot be done then the project cannot proceed, period. Sometimes complex structures will be in place which will make discovering beneficial ownership difficult, particularly in environments where record-keeping and the availability of public information may be poor. Sometimes (in fact, quite often) beneficial ownership will not even appear on any written record, but will simply be a matter of fact or, more often, of rumour. Whatever, if the project is worth it (see later) then persistence must be deployed and beneficial ownership established. Sometimes complex structures deployed to disguise beneficial

ownership may be an indicator of criminal activity (e.g. tax evasion). But equally, they may simply reflect a business reality in the country in question in which business owners must attempt to disguise the full extent of their wealth in order to avoid demands for payments by corrupt officials. So the presence of a complex structure in itself will not necessarily prevent the transaction from proceeding, but lack of knowledge of beneficial ownership will.

Figure 5.3 **IDD process – initial stage**


Start of eligibility review process
Beneficial ownership unknown
Criminal convictions
'Blacklisted'
Credible evidence of criminal associations
Project is ineligible to proceed to next stage if any of these filters apply
Proceed to next stage of the integrity review process

2. No transaction can proceed with parties who have been convicted of, or who are currently under investigation for, serious criminal offences

Serious criminal offences basically mean the predicate offences included in the FATF list of crimes which can give rise to money laundering and constitute, therefore, for example people trafficking and modern slavery, racketeering, corruption and bribery, fraud, tax evasion, counterfeiting, murder and kidnapping, robbery and theft, smuggling, extortion, forgery, piracy, insider trading and market manipulation as well as participation in drug trafficking, money laundering, terrorism and terrorist financing offences. In many countries the presence of a conviction or an ongoing investigation is not necessarily indicative of either guilt or a serious case to answer, as the case may be. Likewise, the absence of a conviction or an ongoing investigation is not necessarily indicative of innocence and/or no case to answer. Issues such as the nature of the crime, how long ago it occurred and whether or not it was politically or commercially motivated will be relevant. But, generally, the presence of a conviction or an investigation will prevent the transaction from proceeding.

3. A transaction cannot proceed if a party is currently on a recognised blacklist

This is self-evident and lists checked would include those of the United Nations, the US Department of Treasury and the Office of Foreign Assets Control, the FBI, the Securities and Exchange Commission, the Financial Services Authority and those of major central banks and other MDBs/IFIs.

4. The transaction cannot proceed where there is credible evidence of existing links to organised crime and criminal activities

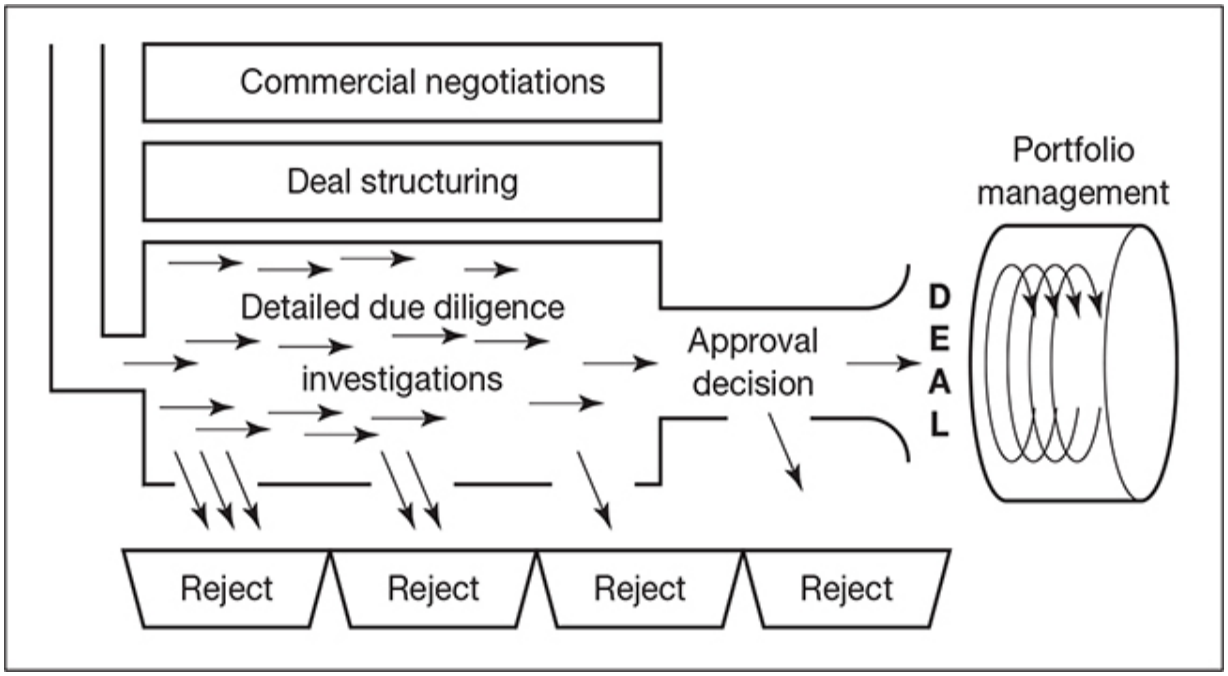
In some instances there will be allegations and rumours that a particular individual or group of individuals are or have been associated with organised crime. Here, the issue of ‘credibility’ is important; the most credible evidence will be that which is corroborated by multiple, independent, impartial sources, as opposed to an allegation made by a

single individual who is, say, involved in a commercial or political dispute with the person in question. The criminal activities referred to are the same as those discussed in item 2, above.

Tax affairs are becoming an increasingly important consideration. Involvement of complex structures and Offshore Financial Centres (OFC) may offend tax evasion laws and, as we have seen, tax evasion is now included in the list of predicate offences issued by the FATF. It is also the subject of an increasingly active and determined international effort, orchestrated through the OECD Forum, to reduce it and to punish tax evaders. Therefore, any complex tax structure must be understood so as to ensure that it does not offend against relevant tax laws in the jurisdictions concerned and any OFC involved must be one which has been deemed compliant with the OECD Tax Forum's international standards on tax information exchange.

If the proposed transaction passes this funnel test, and if it is attractive in other terms (see below) then conceptual clearance is given and more detailed investigations conducted during the secondary stage of the IDD process, depicted in Figure 5.4.

Figure 5.4 **IDD process – secondary stage**



The IDD process: secondary stage

Completion of the red flags checklist at first instance will usually have revealed a number of important issues requiring further investigation. At this stage, assuming all available public sources of information have been accessed using the due diligence resources available (see below), if the transaction is worthwhile in terms of the organisation's mandate then specialist investigations consultants may be instructed to investigate specific areas of concern revealed in the initial research. Here, the assumption is that they will have access to non-public sources of information, although clearly the use and methods of obtaining such information must remain legal. If such investigations harden any of the evidence of the existence of items 1, 2 and 4 above, then a decision is made to drop the project. More often than not, however, despite the added perspective which such investigations usually give, there are no clear answers and a decision has to be made on the basis of the risks versus the mandate.

In this regard reference is then made to the following types of interpretation and assessment principles.

5. Relationships with PEPs and other high-risk clients require enhanced due diligence

The involvement of a PEP does not necessarily prevent the transaction from proceeding, but for reasons examined earlier, it creates notable levels of risk which need to be managed. All PEPs are not equal, and generally the involvement in a business transaction of, say, a head of state, president, prime minister or a senior cabinet minister, as well as governors of large regions and mayors of major cities, is considered too risky and will prevent the transaction from proceeding.

For those PEPs in lower positions, MDB and IFI organisations will generally refrain from transactions if there is an apparent conflict of interest created by a PEP's interest in the business transaction on the one hand, and their public duties on the other: for example, where a minister of transport owns shares in a bus or train company. Compliance with local law is important, as many public sector service rules will prohibit participation by a public servant in a commercial enterprise.

The types of enhanced due diligence investigations regarding source of wealth described earlier on must be undertaken. If a transaction involving a PEP is to proceed, it must also be subject to enhanced ongoing monitoring (to check that the assessment of risks has not changed in the light of new information). The transaction structure should also be constructed with a view to minimising risks. For example, if permitted by local law, the irrevocable transference of share and ownership rights into the control of an independent third party and documented pre-recusals of the PEP from decisions benefiting or potentially benefiting or being perceived to benefit the financed entity. The same rules apply to close family members and associates of PEPs. Arrangements should create genuine independent oversight and not just a documentary fiction.

Although the due diligence resources must be used in order to determine whether or not someone is a PEP, generally this is less of a problem than the bigger issue which is establishing whether or not someone may actually be *fronting* for a PEP. Such situations are common; there is a rumour or an allegation that the disclosed owner of a business structure is not in fact the true beneficial owner, but is fronting for Junior Minister X or Senior Civil Servant Y. In such circumstances, unless the available evidence supports the argument fairly robustly that the rumour is unfounded, then the operation of principle 1 will generally prevent the transaction from proceeding.

6. Mitigating factors can be taken into account when assessing integrity risks

If a particular transaction is attractive from the perspective of the MDB's or IFI's mandate, and if it is not blocked by the operation of principles 1–4, but if there are still concerns about some of the issues which have been discovered during the due diligence process, then mitigating factors can be taken into account when deciding whether or not to proceed. Typical mitigating factors include:

- *Time* – if a significant period of time has elapsed since the last serious allegation.
- *Willingness to change* – cynics may scoff, but there is a view (borne out in part by history) that some business people who have pursued illegal activities previously, do reach a point where they intend to leave it behind them and move on to an exclusively legal future,

unclouded by their illegal past. (The US 'robber barons' of the late 19th century are the classic examples often cited.) If there genuinely appears to be little chance of repetition of illegal activities in the future – say because the amount of a person's reputation and capital invested to date makes the costs too high – then, all else being equal, it becomes possible to take a calculated risk on the individual, subject to the next bullet point.

- *Ability to mitigate risks* – if the applicant is willing, there is often a series of concrete actions which can be taken to mitigate some of the integrity concerns which may have been raised in the red flags checklist. For example, complex ownership structures can be simplified and made more transparent; international accounting standards can be adopted; (genuinely) independent directors can be appointed to the board of a company; a wide range of warranties and covenants can be included within legal documentation requiring the disclosure of wrongful acts and cooperation with investigations by the lender – all linked to events of default which, in turn, are linked to personal guarantees which place personal rather than corporate wealth at stake; and certain companies, individuals (such as agents) and proposed transactional elements can be removed from the deal if they are considered too risky.

If integrity concerns can be mitigated using such methods, then this can result in a move towards a decision in favour of the transaction proceeding. The remaining four principles are effectively operational ones that concern how the inside process must be undertaken.

7. There must be full disclosure of all risks from as early a stage as possible

8. Transactions must be covenanted and documented in a manner which reflects their risk

See 6 above.

9. Integrity risks must be reviewed throughout the life cycle of a project

Information changes over time and risks need to be reassessed and action needs to be taken accordingly. These requirements form an integral part of the portfolio management process.

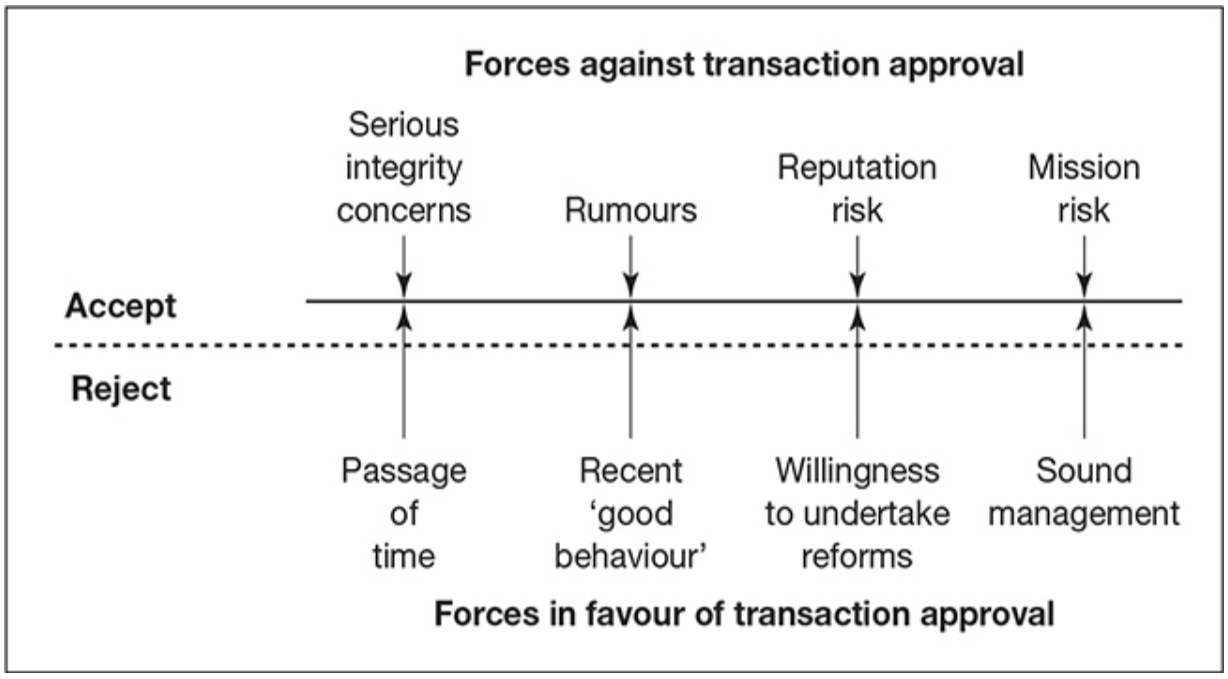
10. Where a project is potentially controversial, a clear explanation of the organisation's rationale for undertaking it should be available

Sometimes, even after the application of sophisticated procedures and thinking, decisions will be made on a hair's breadth one way or the other. No organisation can be expected to get such decisions 'right' 100 per cent of the time. On those occasions when the organisation gets it 'wrong' – and when it is accordingly subject to public criticism – it pays to be able to state very clearly what steps the organisation took to try to get it right, and the grounds on which the decision to lend or invest were made.

The reputational decision which has to be made in each case is summed up in Figure 5.5.

In this forcefield analysis, serious integrity concerns, unproven rumours and allegations, the risks of the organisation's reputation from getting it wrong and the mission risk (objectives not achieved, money not repaid, etc.) are weighed against mitigating factors such as time, recent behaviour, a willingness to undertake reforms, to adopt sound management practices and to accept and embrace mitigation measures.

Figure 5.5 **Forcefield analysis of key factors in IDD decisions**



Each case will be different, but these principles can bring consistency to the analysis. Ultimately, commercial banks operate within their own defined parameters of corporate social responsibility and in order to preserve and enhance their reputations it is against those parameters that they must make their assessments and their judgements.

THE INTEGRITY 'RED FLAGS' CHECKLIST AND THE DUE DILIGENCE INVESTIGATION TOOLS

What types of questions should be asked and hopefully answered during the initial stage of the IDD process? What tools and resources can be used to obtain such information?

Table 5.1 shows, in checklist format, the areas to be covered and questions to be asked.

The past decade or so has seen a significant increase in the capability of organisations to access, and therefore to analyse, publicly available

information through the internet and via various business information products that provide a useful service in information collection and analysis. But traditional methods still count – or should count – for a lot. In all cases, the information needs to be gathered meticulously and either copied and placed on file together with the data research, or recorded as a contemporaneous note. Table 5.2 lists a range of due diligence tools.

Table 5.1 Example 'red flags' checklist

Project background
A. Is the company private or public? Are there any risk implications? B. What is the industry of operations of the company? Are there any risk implications? C. What is the country of operation of the company? Are there any risk implications?
Category 1: Criminality, criminal associations and convictions
1. Have the proposed senior management or co-owners of the company ever been convicted of a criminal offence? 2. Have they been or are they under investigation by law enforcement agencies? 3. Have they ever used criminal means (e.g. blackmail, intimidation)? 4. Have they ever been involved or associated with criminals? 5. Have they ever been involved or associated with money laundering?
Category 2: Bribery and corruption

6. Have they ever been involved in the misuse or misappropriation of public property?

7. Have they ever been involved in bribing public officials to influence public decisions or processes?

8. Has there been any involvement in business sectors frequently characterised by corrupt practice?

9. Are there any unexplained pools of cash or near cash investments in the company's or senior managers'/co-owners' finances?

10. Have there been any inappropriate or above-market economics, fees or local costs in the company's activities?

11. Have there been any instances of transfer pricing, bid-rigging or financial misrepresentation?

12. Are there any unknown or suspicious sources of wealth?

13. Do any of the senior managers/co-owners display an ostentatious lifestyle which appears to be inappropriate to their financial situation?

14. Are they reluctant to discuss integrity or corruption issues?

Category 3: Political exposure

15. Do any of the senior managers/co-owners have major political affiliations or have they made political financial donations?

16. Are any politicians or government officials involved with the company, e.g. as directors or beneficial owners?

17. Are any of the owners/senior management from ‘political families’ within the country concerned?

18. Are any of the owners or senior managers known members and supporters of extremist political or religious groups?

Category 4: Beneficial ownership and corporate governance

19. Have the senior managers/co-owners of the company ever committed fraud or misappropriation of assets against shareholders?

20. Are there any undisclosed or unusual beneficial ownership or carried interests?

21. Have there been any sudden or unexplained withdrawals of large and/or western companies from transactions?

22. Have there been any sudden or unexplained changes of shareholders, auditors, accountants, lawyers or other professional advisers?

23. Are there any unnecessarily complex ownership structures?

24. Has there been any tax evasion by the company or the senior managers/co-owners?

25. Are there any ‘suspicious’ (seemingly unnecessary) offshore companies within the corporate structure?

26. Has there been any non-market compensation of key participants, such as the company itself, the senior management/co-owners or other shareholders?

27. Have there been any other examples of poor corporate governance?

Category 5: Regulatory investigations, fines and lawsuits

28. Have there been any large or serious lawsuits, fines or regulatory or public findings which have impacted negatively on the reputation of the company or the senior managers/co-owners?

29. Are there currently any outstanding large or serious lawsuits or regulatory or public investigations which remain unresolved?

Category 6: Personal and corporate reputation (including blacklisting and press/media reports)

30. Do any of the senior managers/co-owners appear on any UN List of persons suspected of involvement in terrorist activities or any other watchlists referred to by the Bank (e.g. US Dept of Treasury, OFAC, SEC, FBI, EU, FSA (UK), HKMA (HK))?

31. Have there been any media references to illegal or disreputable activities or actions or any actual evidence of the same?

Table 5.2 Due diligence tools

- Searches of newspaper and business publications and websites

- Searches of society and sports magazines (e.g. sailing, polo, philanthropy) and websites, where relevant
- Informal discussions with industry, sector and country contacts
- Checks with foreign banks and other foreign companies who may be able to give an informed opinion
- Searches of relevant public information and private subscription search engines and websites, such as Google and World-Check
- Searches of open source databases such as Wikileaks and the Panama Papers
- Searches of public registries and record offices (to the extent that these are deemed sufficiently helpful and reliable) in the country or countries concerned, such as companies' registries and court and judicial offices
- Structured discussions with the applicants themselves
- Investigations by specialist firms of investigations and OSINT consultants (For an intriguing information source on these arts, visit www.bellingcat.com)

PRACTICAL APPLICATION

How might this overall framework apply in a real case? What would the file look like in terms of relevant information and how would the IDD assessment guidelines operate in practice?
We attempt to bring this to life in the form of a fictitious case. First read the project summary to get an initial outline of the proposed project and then access the types of information which you would obtain on such a case were you handling it for real and using the research tools referred to above. Finally, there is an assessment of the project according to the assessment guidelines discussed.

Case: Zubin Deslan and the Belvin Keffl Group

Project summary

- Belvin Keffl (BK) is a former state-owned farming company in the EU candidate country of Moldavia.
- BK diversified after the fall of communism into areas such as food, transport, chemicals, retail and construction.
- It was privatised in 1991 and became owned by the Deslan Group of companies, whose majority shareholder, chairman and chief executive is Zubin Deslan.
- The proposal is for loan financing for the general upgrading and expansion of Belvin Keffl's truck production facilities in the major cities of Krestinberg and Bantt, which used to produce the old 'Paka' state trucks and buses.
- The amount of the proposed investment – €20 million – is to be spent on factory and plant rebuilding using capital equipment purchased from member countries – notably from the Finnish engineering giant, Sarbel Engineering.
- The project has been brokered through the auspices of Peter Valburg, a former Sarbel employee now based in Moldavia and used as an independent consultant throughout the region.

Commercial viability of the project

Commercial viability is good. The market for trucks is likely to remain strong as this robust emerging country continues to grow and the government is a major customer with a constant need for fleet upgrading and renewal. As an oil exporter Moldavia is likely to benefit from high oil prices and this will benefit the economy as a whole. Market research indicates that executives in Moldavian companies are quite patriotic and are prepared to back a national champion if it meets reliability requirements, particularly in the snows of winter, which is where the use of Finnish expertise and *matériel* will become most useful. Costs are predicted to grow by 6 per cent a year, while revenues are estimated to grow by 25 per cent year on year as the business development plan unfolds. There are considered to be potential regional export possibilities, too.

Compliance with environmental policies and strategies

Like many engineering production facilities within the former Eastern bloc, BK has suffered from chronic underinvestment, dangerous, outdated facilities, health and safety issues for employees, and high pollution levels, with associated contamination of air, rivers and countryside around the plants. An attractive feature of this project will be bringing the plants up to the latest international standards in these respects.

Moldavian overview

Moldavia has 20 million people, set to grow to 30 million by 2050 with oil and mineral resources. Moldavia is a vast, untapped country which is likely to grow in stature and become a major regional player. It is modernising rapidly and the view is that it is a good country for business, with the current government, formed by the Moldavian National Progress Party (MNPP), apparently committed to the implementation of a full set of market reforms with a view to securing EU membership by 2025. Despite a plethora of government backed initiatives, corruption, however, is still viewed by many foreigners as endemic in everything from the award of business contracts, to the making of regulatory decisions, to the securing of preferment and promotion in both the private and public sectors.

There is a crime problem in Moldavia. It is improving but organised crime undoubtedly exists and the use of intimidation, violence and even murder to resolve political and business disputes, while much less common than it was during the 1990s, still occurs from time to time.

Deslan Group overview

The group is substantial in national terms and has shown a strong business performance over a sustained period. There has been undisturbed profit growth year on year since 1993 and an aggressive acquisitions strategy has seen core businesses grow rapidly, particularly following the hard-fought acquisition of AIA Group in 1994. Construction and transport still contributes more than 50 per cent to profits, helped no doubt by continued good relationships with the public sector. The strategy is to continue to grow these businesses strongly, leveraging their excellent market positions, as well as the renewed focus on the trucks business.

The group is organised through a series of divisional structures, with operating companies owned by a series of holding companies, which in turn

belong to the main holding company, Deslan Holdings, which is believed to be 80 per cent owned by Zubin Deslan and various family members, all of whom operate through nominees (i.e. legal entities such as companies and trusts which hold on behalf of a beneficial owner). Corporate administration appears sound, with all books up to date, meetings held and minuted, all returns filed within time and no fines or other censure or criticism from the Moldavian Corporate Authority (MCA).

Financially the group appears strong and although it undoubtedly has the funds to finance the proposed project itself, this would mean that it could do virtually nothing else – a situation that makes no sense at all given the multiple opportunities the group is presented with.

Zubin Deslan

Born in 1961, Deslan is the son of a university professor and a teacher and has five siblings. He is quiet and non-demonstrative – not your average - Moldavian businessman, who tends to be a 'larger than life', street trader, *bon viveur* type. He got a first class honours in Biochemistry from Krestinberg University, followed by two years' national service in the air force, 1983–85. His career in the Ministry of Agriculture culminated in a position as a director general of Belvin Keffl in 1989.

Deslan bought Belvin Keffl from the Moldavian government in 1991 (aged 30) apparently using finance raised from contacts he made on a short-term summer management programme at Stanford Business School in the late 1980s and grew the business from then into the conglomerate which it is today. He has successfully raised funds from FFIs in the past, including from Goldman Sachs and UBS. His acquisition of AIA Group in 1994 was bitterly contested and controversial at the time, as victory effectively handed Deslan control of the food and agricultural sectors in Moldavia, as well as giving him a substantial slice of the chemicals and construction sectors. Both Deslan personally and Deslan Group, were financial contributors to the ruling MNPP who won last year's elections on a wide-ranging (and popular) programme of reform and liberalisation based on getting people to consign the country's poverty-stricken communist past to the history books, and unite around a bright and prosperous future. The MNPP is bitterly opposed by the other main political party, the Moldavian People's Power Party (MPPP), which claims that modernisation has been a

disaster for the poorest, and advocates a more state-led approach to the economy to protect wages and living standards.

Information 1 – obtained from a public registry

COMPANIES REGISTRY OF MOLDAVIA

CERTIFICATE: DESLAN HOLDINGS PUBLIC COMPANY
Breakdown by owner category of numbers of shares held

A. Other listed private sector companies – 0
B. Private individuals – 0
C. Publicly owned bodies – 0
D. Nominee companies – 5,625,766

Information 2 – obtained from the website of Transparency International

Relevant sections from Transparency International's Anti-corruption Index, contained in its latest annual report (1 = least corrupt):

123.Moldavia

124.Bulgaria

125.Ukraine

126.India

127.Pakistan

128.Indonesia

Information 3 – obtained from a conference call with the country manager, who obtained it orally from an attorney friend

Note

20/8

Telephone conference call with our local manager, who has been speaking to a local investigator and has uncovered the following information:

- Deslan investigated twice, both times no charge
- 1) In 1996 re privatisation of BK in 1991. Alleged bribery of State official, Henrik Bolsan, responsible for sale, but *NOTHING PROVEN.*
- 2) In 1999 re allegations that BK/DG acquired AIA Group illegally in 1994 via secret agreement with CEO Georges Vandreau who pushed through sale at undervalue in exchange for a $12m payment to an offshore bank account. *NOT PROVEN.*
- Investors in AIA lost €€€ millions on sale after collapse of investment scheme promoted by Vandreau. V based in London 10 years – old man and died of cancer just before election last year.
- No further investigations. Police files on both cases above now closed. Reason given – *NO EVIDENCE.*

Information 4 – obtained from a local newspaper by the country manager

Handwritten note faxed over by local manager

Deslan and Deslan Group are donors to the MNPP and he does a lot of this kind of thing with them, as indeed do many Moldavian businessmen. But I thought you should be aware of it. Regards, JL
17/8

Information 5 – obtained from an international newspaper

FINANCIAL NEWS

But Moldavia may yet come to terms with its tumultuous past and, in particular, construct a permanent settlement between the state and the private sector concerning the corrupt and self-serving ways in which state assets were sold off after the demise of communism.

PAY YOUR TAXES

The recent statement by Finance minister Egbert Aldoa is a case in point. In a wide-ranging interview for CNN Business, he indicated that the Moldavian Government would no longer be looking to prosecute cases of alleged acquisition at undervalue historically, as long as those suspected behave as good corporate citizens and pay their taxes here and now in the 21st century.

One person who will welcome such statements is undoubtedly Zubin Deslan, creator and CEO of the eponymous Deslan Group, a sprawling Moldavian conglomerate which is into everything from food and agriculture to mines, construction, chemicals and trucks. The previous government tried unsuccessfully to bring corruption charges against him and Agriculture Secretary Henrik Bolsan in 1996 in relation to Deslan's acquisition of the state-owned Belvin Keffl Group (a decision signed off by Bolsan) but these failed due to lack of evidence and Aldoa's ruling MNPP has shown succumbed to terminal cancer last year and Deslan is both an eloquent and generous supporter of the ruling MNPP party.

RIGHT TRACK

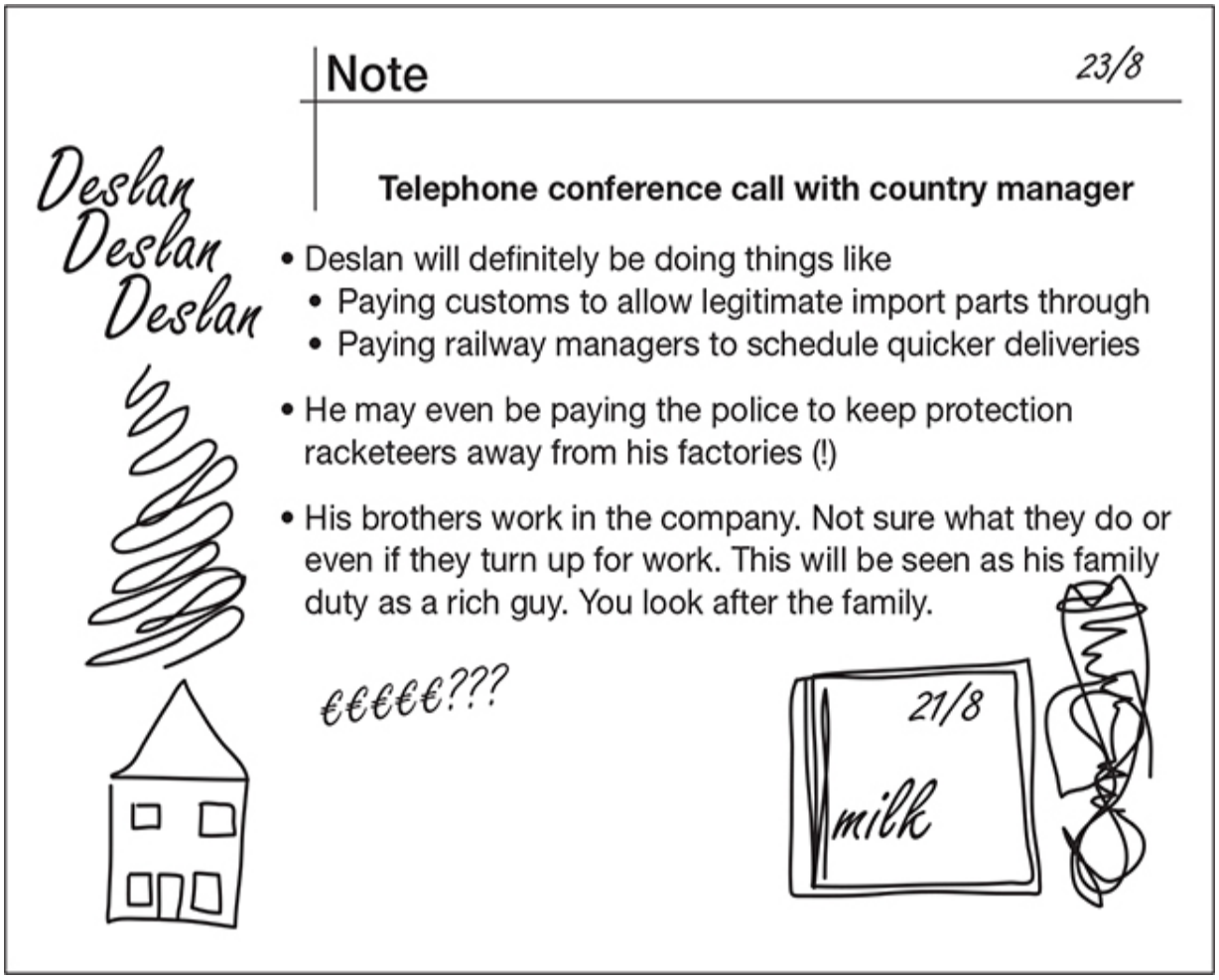
Those close to the Moldavian political and business elite now believe that if the country can cement this settlement and continue with the economic reform programme, then the future would be bright, heralding prosperity and, whisper it softly, even power.

"Moldavia has some of the largest oil reserves in the region", says Patrick Climbe, Head of the Economic Research Institute in Krestinberg. "It has minerals, a sizeable population that is set to be larger than Canada's by 2050, and is well placed politically to join the modern economically developed world."

But others are more sceptical and point to rampant corruption, a simmering historical enmity with neighbouring Moldachia, and an opposition party which is far from weak and which is itching to return to power and settle some old scores. "Moldavia is only ever one election away from a return to state economics and a catastrophic war with Moldachia" says Prof. Marian Divlas of the Chair of international studies at Krestinberg University. "That's what I tell anyone who starts

little appetite to resurrect the case, especially since Bolsan himself getting too starry-eyed about the future."

Information 6 – obtained by country manager from local business people


Note
23/8
Telephone conference call with country manager
Deslan
Deslan
Deslan
• Deslan will definitely be doing things like
• Paying customs to allow legitimate import parts through
• Paying railway managers to schedule quicker deliveries
• He may even be paying the police to keep protection racketeers away from his factories (!)
• His brothers work in the company. Not sure what they do or even if they turn up for work. This will be seen as his family duty as a rich guy. You look after the family.
€€€€€???
21/8
milk

Information 7 – obtained from the legal department via local lawyers after analysis of the company's constituent documents

Confidential Memorandum

LEGAL; PRIVILEGED AND CONFIDENTIAL

The Bank's lawyers in Krestinberg, Messrs Panaca Dale, have provided the following assessment of the corporate governance levels of both BK and Deslan Group. Please note that this is the initial assessment and is subject to any further information provided by the company.

"The legal framework and company charter provide for basic shareholders' rights such as the registration of shares in share registers, the right to transfer shares, to participate in general shareholder meetings and to elect and dismiss board members. However, there are no sufficient mechanisms to ensure protection of such rights or redress in cases of violation. Minority shareholders are not necessarily granted equitable treatment (e.g. the voting rights of different classes of shares are not well defined, insider dealing is not properly regulated, etc.). Stakeholders' rights are not necessarily recognised. There are certain disclosure requirements of material information on the company, which however do not allow shareholders to get a thorough understanding of the financial situation of the company, with such information being provided on an infrequent basis. There is little transparency to third parties, which are given limited access to company financial information or its ownership structure. The company board is required to have some degree of accountability to shareholders, although the enforcement mechanisms of such requirement are overall ineffective."

I would add two more things:

The actual shareholdings of Deslan and his family appear to be through nominee companies, meaning less transparency all round.

In this regard I am led to believe that Mr Deslan himself is prepared (even keen, some say) to follow any suggestions we may make regarding the creation of greater transparency (real and perceived).

I think an early meeting is in order.

Sincerely,

Kate Bryan

Senior Legal Advisor

Information 8 – obtained from the local public registry

22 Krestinberg Square
Krestinberg 20098
Republic of Moldavia

Fax Transmission

To: Project Team
From: Jan Larsson, Representative Moldavia
Re: Belvin Keffl
Date: 20 August

MESSAGE
As requested I have conducted a search of the newly completed Moldavian National Criminal Archive, which reveals NIL convictions for either Deslan, his known family members or any of his senior management.

Best regards,

J. LARSSON
Representative, Moldavia

Information 9 – obtained from an industry contact

Transcript of telephone conversation with Alan Greenton, a business acquaintance and former US banker with a good knowledge of Moldavia

YOU: What can you tell me about Peter Valburg?

GREENTON: Peter Valburg? Oh I know Valburg quite well. There are a few of these guys knocking around in Krestinberg and Valtana [capital of neighbouring Moldachia] and, well, what can I say? They're very well connected, they know a lot of people and many would say – and they themselves would say – that they provide a valuable service to people wanting to do business in Moldavia for the first time. They make the introductions, they negotiate the labyrinth of regulations, they know about starting an operation, investment rules, local taxes, etc. etc. Cynics, of course, would say that they're just there to make the FPS (facilitation payments) and, where necessary, the bribes, and to provide the necessary tax deductible invoices to western companies … And of course, they're working it both ways. As westerners, they can hop on a plane back to Copenhagen or London or New York or wherever and sell the best deals to the highest bidder …

YOU: So he's corrupt.

GREENTON: Well, what's corrupt these days? Is he walking into the prime minister's office with suitcases full of cash? No, of course he's not. But if a local manufacturer with some easy government contracts needs western capital equipment and a guy like Valburg sets up the deal with, say, the British company which was willing to make the largest 'thank you' payment, and they get some western bank to finance the whole thing, well is that corrupt? You tell me …

Information 10 – obtained from a Google search against 'Sarbel'

Sarbel bribes reached around the world

Evidence from key witness details millions of euros paid in bribes to officials in Nigeria, Russia and Libya

Sarbel, the engineering group at the centre of the biggest bribery scandal in Finnish corporate history, paid millions of euros in bribes to cabinet ministers and dozens of other officials in Nigeria, Russia and Libya.

The payments were made as the company sought to win lucrative contracts for engineering and transport equipment, according to court documents revealed in *The Wall Street Journal* today.

A ruling by a Helsinki court last month names four former Nigerian telecommunications ministers as well as other officials in Nigeria, Libya and Russia as recipients of 77 bribes totalling about €12 million (£8.6 million). Sarbel accepted responsibility for the misconduct and agreed to pay a €201 million fine decreed by the court.

The court focused on bribes between 2001 and 2004 connected to Kiki Rakkinen, a Sarbel employee who was a manager in a sales unit.

Mr Rakkinen has been charged with embezzlement and is cooperating with prosecutors.

According to separate court documents, Mr Rakkinen has told prosecutors that he knows about bribes beyond Nigeria, Russia and Libya, that were made with the knowledge of senior managers.

His evidence could lead to other criminal investigations and additional fines in other countries where Sarbel is active, including the US.
Mr Rakkinen alleges he has knowledge of corruption involving Sarbel managers in more than a dozen countries, including Brazil, Cameroon, Egypt, Greece, Poland and Spain.

If Sarbel is found to have acted corruptly in certain other countries, including the US, it will also face bans on public-sector contracts.

Last week, Sarbel said that it had largely finished its internal investigations and had found €1.3 billion in suspicious payments for tax purposes and that the scandal had cost it €1.3 billion–€1.4 billion so far. The CEO, Per Anders, has resigned and the company has undergone a board

CEO, Per Anders, has resigned and the company has undergone a board shake-up and a complete reorganisation of its compliance function.

Case analysis

Using the integrity risk management framework described earlier, an analysis of the above due diligence information would reveal the following core issues:

- *Initial finance* for the purchase of Belvin Keffl – how was this raised, who from and what were the terms? Was the initial source of wealth therefore legitimate? *Further investigations would be necessary*.
- *Beneficial ownership* of the Deslan Group and Belvin Keffl. Are Deslan and family really the owners? Could they be fronting for others (e.g. political friends)? The nominee structure has the effect of hiding ownership. What about the 20 per cent that is not in Deslan's hands: who does that belong to? *Further investigations would be necessary. Failure to obtain comfort on beneficial ownership would offend against principle 1 and prevent the deal going ahead*.
- *Bribery allegations on (1) the Belvin Keffl purchase and (2) the acquisition of AIA Group.* The absence of criminal trials and convictions is still not necessarily evidence of innocence in a country like Moldavia. Also, both men who allegedly took bribes from Deslan have recently died, albeit from apparently natural causes (cancer). *Further investigations would be necessary, but probably not much more could be found out about this*.
- *Political connections*. Deslan is very close to the ruling party and is a financial donor. This exposes business relationships between them to allegations of corruption and conflicts of interest, particularly since Belvin Keffl enjoys the benefit of government truck contracts. It is also possible that Deslan would become a target of the main opposition party if it achieved power, and could then reopen investigations against him.
- *Poor business practices and poor corporate governance*. Corporate governance is poor, with no independent oversight of the board and inadequate financial information, which is a credit and a fraud issue as much as an integrity and corruption issue. Apart from

the major bribery allegations referred to above, the information reveals with some certainty that Deslan and his companies engage in a variety of practices ranging from the making of facilitation and other unorthodox payments to police and officials through to the awards of contracts and jobs on the basis of family and friendships rather than on merit. *Many countries now make no distinction between bribes and facilitation payments. If the allegations are believed to be true, and the activities are ongoing, with no prospect of cessation then this would offend against principle 4, notwithstanding the absence of a conviction, and would prevent the deal going ahead*.

- *Sarbel Engineering and Peter Valburg*. A proposed beneficiary of the financing, Sarbel, has recently been subject to a media storm in relation to proven bribery and corruption allegations across its global operations. Nevertheless, Sarbel is also one of the largest corporations in Europe, has removed its chairman and CEO and has embarked on a substantial anti-corruption programme to 'defumigate' the company and bring it into line with required international standards. It does not help, however, that Sarbel has been introduced to this business by Peter Valburg, who one source claims is possibly engaged in brokering payments for business, kick-backs and the negotiation of contracts at non-market rates. *Peter Valburg would have to be removed from the transaction*.

In mitigation of all of the above, the acquisitions of Belvin Keffl and the AIA Group took place a long time ago. Deslan appears willing to adopt better corporate practices and it is possible that he has 'moved on' from the worst excesses of his early career. He is not blacklisted and there are no allegations that he has ever been involved with organised crime or money laundering. If the beneficial ownership issue could be resolved and some real comfort gained that he had ceased making facilitation payments to minor officials, then given the absence of any convictions for serious crime, that would mean that he would actually be capable of passing the 'funnel tests' currently operated by the MDBs. In addition, following further investigations (almost certainly using external specialist investigations firms and tools) it would be for the lender to weigh up the uncertainties against the benefits, in light of the mitigating factors referred to, plus any

relevant covenants, undertakings, representations and warranties which could be incorporated within the deal documentation, such as:

- a corporate restructuring to flatten the ownership structure and make beneficial ownership clearer and more transparent
- a corporate governance overhaul to provide protection for minority shareholders and improve access to company information; also the adoption of international accounting standards and the appointment of independent directors to the board
- undertakings by owner and management not to engage in corrupt and illegal practices (as defined) – linked to events of default and personal guarantees connecting default to personal wealth
- undertakings by owner and management to report immediately instances of actual or suspected fraud or corruption
- representations denying the historical allegations of bribery and disclosing the source of the initial wealth used for the purchase of Belvin Keffl – again linked to events of default and calls on personal guarantees should these subsequently be proven to be untrue.

6

Suspicion Recognition

Background and general principles

Money laundering typologies

Terrorist financing typologies

Account analysis examples

'Accumulation of evidence' cases

The 21st century: areas of rising concern

BACKGROUND AND GENERAL PRINCIPLES

A critical requirement for financial institutions and others charged with responsibilities for the detection and prevention of money laundering and terrorist financing is that they report instances where they have become

suspicious that their facilities and/or services may be being used for criminal purposes (see Chapter 2). This requirement begs the twin questions of what it means to be 'suspicious' and under what circumstances a person should be *deemed* 'suspicious'. Or, putting the issue another way, when does it become *un*reasonable for a person *not* to be suspicious?

It is possible to view 'suspicion' as lying somewhere in the territory between *speculation* and *belief*, on a spectrum of awareness with *ignorance* at one end and *knowledge* at the other (see Figure 6.1) .

An English judge, interpreting national legislation, has described it thus:

> **'A degree of satisfaction, not necessarily amounting to belief but at least extending beyond speculation, as to whether an event has occurred or not';**

And

> **'Although the creation of a suspicion requires a lesser factual basis than the creation of belief, it must nonetheless be built upon some foundation'.**

Source: JMLSG Guidance 2017, Part I, 6.11 (from http://www.jmlsg.org.uk/)

At certain points, therefore, it becomes unreasonable either to suspect or not to suspect somebody of something.

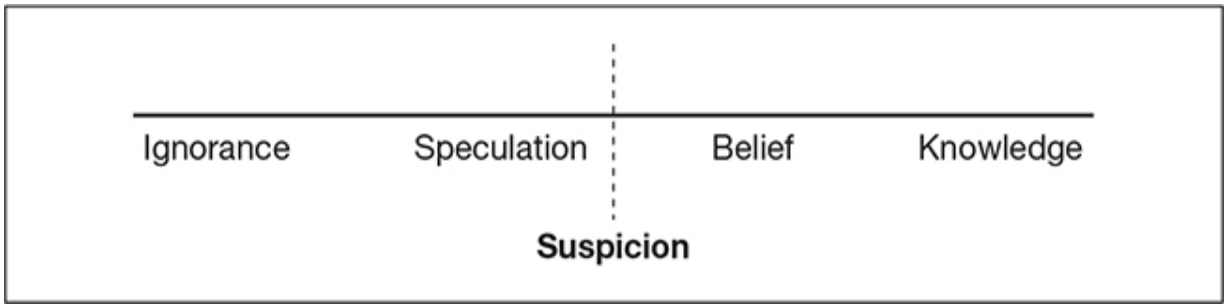
So, at what point is it reasonable to become suspicious?

Example

'S' was a getaway driver on a burglary whose defence in court was that he hadn't known that he was taking part in a burglary – he thought he was simply driving some friends to and from a business meeting that they were attending at a private residence.

In convicting him of aiding and abetting, the jury rejected this on the grounds that his accomplices had put stockings over their heads and armed themselves with batons, jemmies, holdalls and a variety of other tools prior to exiting the car he was driving ...

Figure 6.1 **The 'suspicion spectrum'**



Applying the above reasoning to a terrorist financing case, clearly it is unreasonable to suspect a person of being a terrorist or a financier of terrorism simply because they are from an ethnic group which has terrorists operating within it. Likewise it is unreasonable *not* to suspect a person of money laundering if they were receiving millions of dollars through their account each month, when their annual salary was $30,000 and there was no credible reason for the activity on the account.
Is the test for suspicion under law 'subjective' or 'objective'?

Example

Alicia is a relationship manager in the AlnaBank corporate division. Her customer, Amwell Trading, has an office in Columbia from which it remits frequent large sums of unknown origin to its UK account, which are then wired straight through to the account of another company at a bank in an offshore location, purportedly in respect of debts owed to that company by Amwell. She files no suspicious activity report because she is not suspicious. Suddenly, the company's accounts are frozen under a court order as being criminal proceeds from Amwell's suspected drugs operation and Alicia is interviewed by the police. She agrees to submit to a lie detector test, in which she is asked, 'Did you at any time suspect that Amwell might be engaged in criminal activity?' She answers, 'No' and

passes the test. But colleagues, advised of the facts, state that they would have filed a report had they been managing the account.

In fact, having originally been subjective, the test for bank staff reporting suspicions is now generally an objective one. In other words, it does not matter that you yourself (like Alicia, above) were genuinely *not* suspicious about a client's activities. If reasonable people in your position, knowing what you knew, *would* have been suspicious, then you will have fallen short of the required standard of vigilance if you yourself do not suspect.

The typologies

In the remainder of this chapter, a wide variety of different money laundering and terrorist financing typologies and methodologies are described and depicted. The methods shown are by no means exhaustive, but they do constitute a wide-ranging collection from multiple sources.

The Financial Action Task Force (FATF) regularly publishes reports of the latest methodologies or 'typologies' being used by money launderers around the world. In each case the method is described, followed by an analysis of its key features, its attractiveness from the launderer's perspective and a summary of the warning signs or 'red flags' that might alert staff to potential money laundering or terrorist financing.

FATF has published a number of these reports on general typological trends. In addition it has been very active in recent years in researching areas of specific risk and has published further reports targeting such risks.

Developing skills in recognising typologies

Knowing the signs of potential money laundering and terrorist financing is arguably the single most important capability which staff within financial organisations should have. Accordingly, through training and awareness programmes, Compliance Officers must ensure that staff know what they are looking for in a suspicious transaction.

In our company, Lessons Learned Ltd, we have developed a number of tried and tested training techniques which we use with client organisations to raise awareness and understanding of different typologies and how to recognise them. We have provided examples of three of these techniques

below in our descriptions of different typologies. The training techniques in question are:

- three-part slide presentations
- account analysis practice exercises
- 'accumulation of evidence' case studies.

All these can be complemented with online videos to add interest and engage staff with the issues.
Also included in this chapter is a section on rising areas of concern for the 21st century, covering cases and potential red flags and suspicion indicators in relation to modern slavery, cryptocurrencies and grand corruption.

Three-part slide presentations

Discussions focus on a specific typology and are based around three presentation slides. The first of these provides an animated explanation of the typology and how it works. The second slide lists key facts about the typology. The third and final slide lists 'red flags' to look out for as possible signs of the typology in action. The three slides can be used either for a straightforward presenter-led explanation of the typology, or they can be linked to discussion questions such as, for example, 'How does typology X work?', 'What is attractive about it from a money laundering perspective?' and 'What red flags or indicators might make you suspicious that this typology is being used?'

Account analysis practice exercises

Participants are given printouts showing sequential transactions on an account. They work in groups to identify and explain potentially suspicious features in the transaction patterns shown.

'Accumulation of evidence' case studies

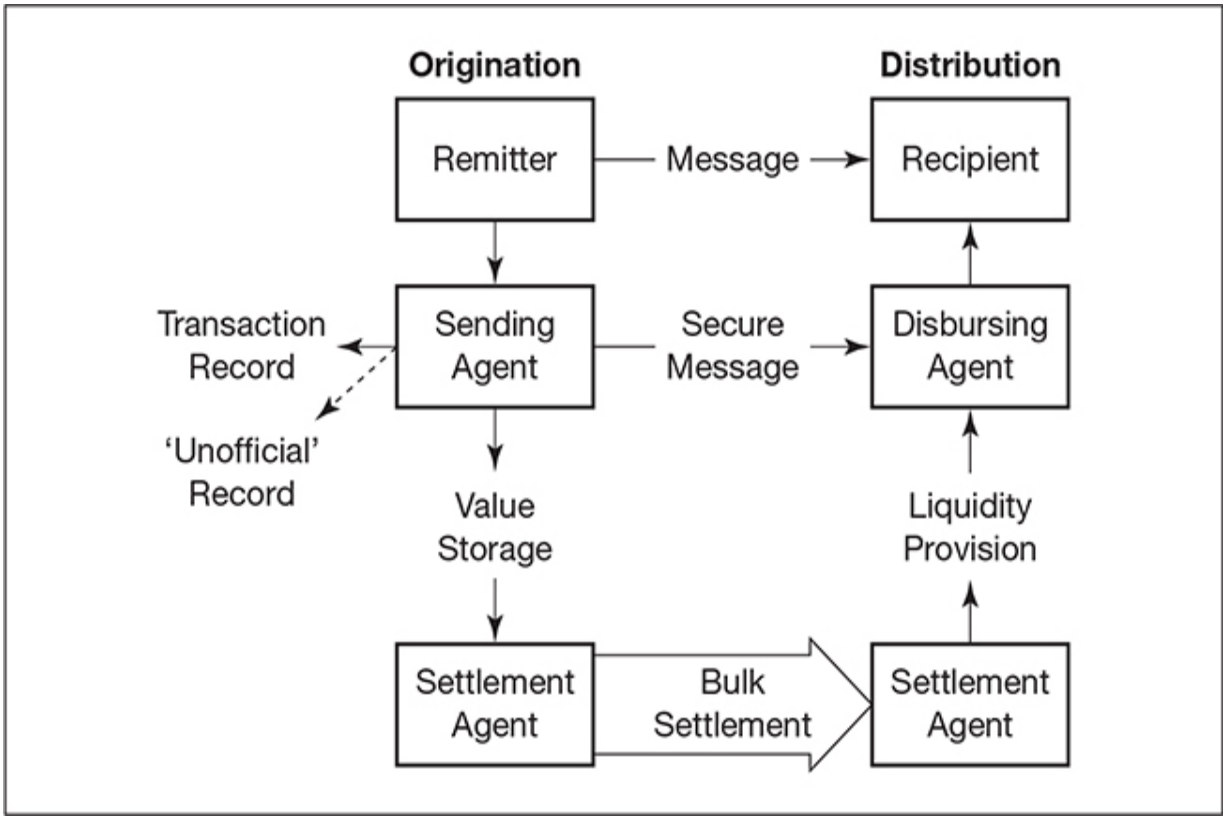
Participants are given some initial information about a client and their relationship with a financial institution. They are given further bits of information one at a time which, eventually, should start to raise concerns, points of doubt and possible suspicions regarding the client's activity within the relationship. The use of such case studies can demonstrate how the nature of relationships can change over time, with initially innocuous

relationships becoming unusual and potentially suspicious as new behaviours emerge.

MONEY LAUNDERING TYPOLOGIES

Alternative remittance services

Alternative remittance services



Source: © Lessons Learned Ltd 2019

How they work and potential for misuse

1. The remitter instructs the sending agent to make a remittance and deposits funds with it, often in cash.

2. The remitter may send its own message to the recipient independently of the sending agent, to alert it to the fact that money is on its way.
3. The sending agent contacts the disbursing agent with instructions to issue funds to the recipient, which the disbursing agent duly does.
4. The sending agent makes a record of the transaction, and the remitter's funds sit in storage, accruing value and ready to complete the settlement via a settlement agent (if one is used).
5. The sending agent either issues funds directly or via a settlement agent to the destination country, where the money is held in storage and available for use.
6. On receipt of the settlement funds the disbursing agent is reimbursed for the funds issued and the transaction is complete.
7. Problems arise when the settlement amounts are transmitted as a bulk transfer, in which case it is relatively easy for laundered funds to be hidden in with the legitimate ones.
8. Unscrupulous ARS operators may also keep a separate 'unofficial' record of these covert transactions, this unofficial record being maintained separately from records of legitimate transactions.

Key facts

Alternative Remittance Service (ARS) is a term which can describe any system for transferring money outside of normal banking channels. There are many perfectly legitimate ARS operators as well as a few rogues. There are often ties between certain systems and particular geographic regions, and such systems are often described using a variety of specific terms including *hawala*, *hundi* and *fie-chien.*

It is clear that the vast majority of people who use ARS operators are perfectly ordinary and law-abiding with no criminal intentions whatsoever. There are a number of legitimate reasons for such people to want to send money via an ARS operator rather than through normal banking channels, for example:

- *Reasons of accessibility*: many people are denied access to normal banking facilities because of where they are based geographically, or because of their personal creditworthiness; these people have no choice but to use ARS operators to send money.
- *Cultural familiarity*: in certain parts of the world (e.g. many parts of the Middle East and Asia) systems such as *hawala*, *hundi* and *fie-chien* are culturally perfectly normal and may well be chosen in *preference* to the normal banking system.
- *Personal contacts*: extended families spread across the world may often use informal agreements to exchange money on behalf of friends and associates who require money to reach a particular person perhaps more quickly than the banking system can arrange; there is nothing illegal in what these people's contacts do for them, they are just being pragmatic and helpful.
- *Speed*: as explained above the banking system is not always fast enough, and informal arrangements via networks of associates can offer a quicker service where one is needed.
- *Anonymity/secrecy*: clearly remittances that bypass the normal banking systems can be carried out in relative anonymity and secrecy, and it goes without saying that this is why money launderers find the ARS systems attractive.

Money launderers' perspective

The attraction for money launderers is, as stated above, the opportunity for concealment that ARS can sometimes offer. ARS operators are generally unregulated and not subject to scrutiny by the authorities. The operators themselves often use codes in their records rather than specific individuals' names, and this also aids concealment.

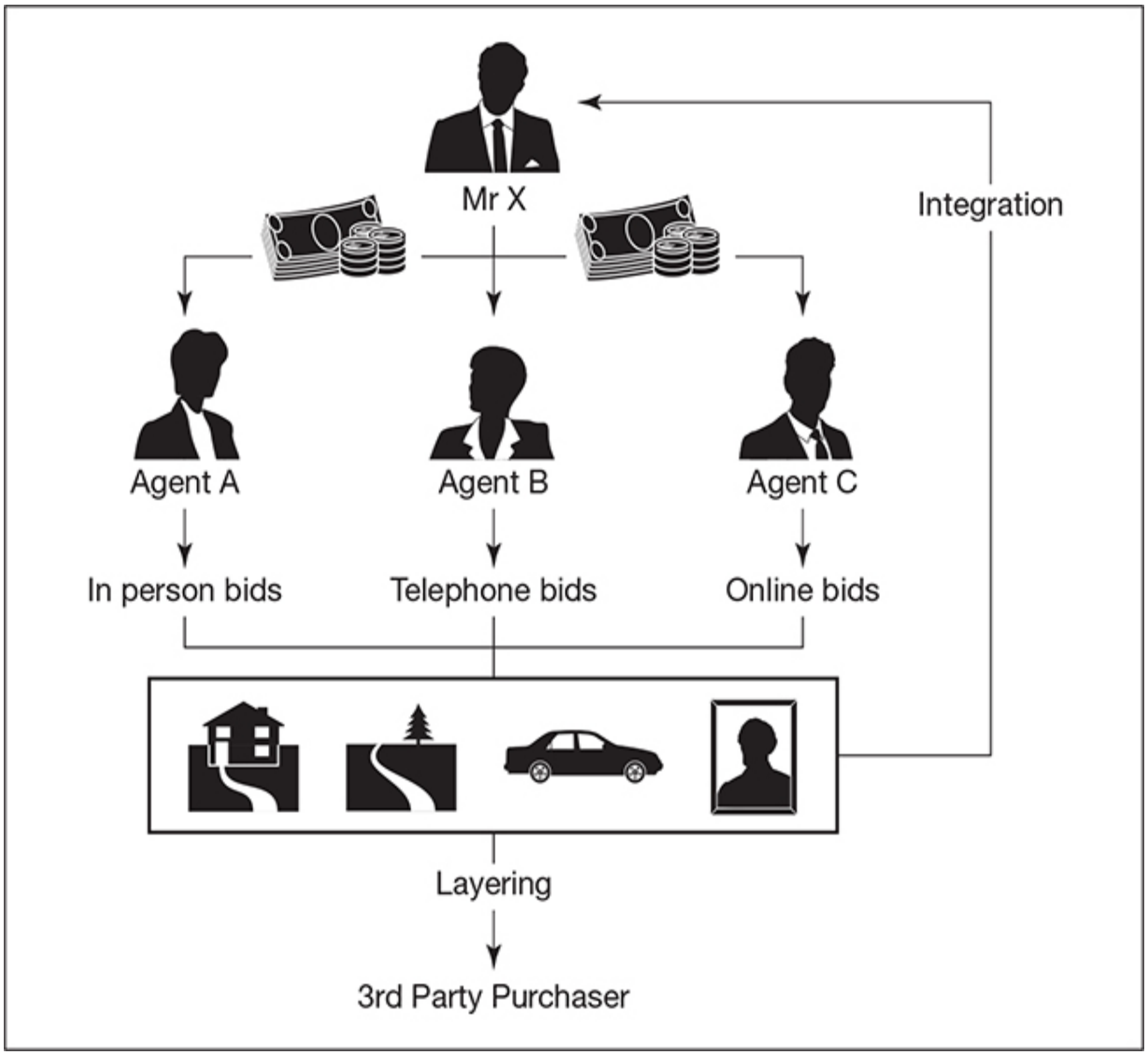
Possible red flags

FATF has identified a number of possible suspicion indicators which might indicate that an ARS operator's business is being used for money laundering. Indicators include:

- remittances in excess of the norm for the customer's known economic background
- unusual escalation in levels of remittance for an individual
- personal remittances sent to destinations that do not have an apparent family or business link
- remittances made outside migrant remittance corridors
- reluctance of customer to give explanation for remittance
- personal funds sent at a time not associated with salary payments
- requests for a large transfer but settling for smaller amounts – - potential structuring.

Auctions

Auctions



Source: © Lessons Learned Ltd 2019

Money laundering via auctions

1. The launderer distributes the cash proceeds of crime to a network of agents. Agents either retain the proceeds in cash form or bank the cash in own name bank accounts.
2. Agents go to auction and bid via whatever means is necessary, i.e. in person or over the telephone via another third party at physical auctions or electronically for online auctions.
3. Agents bid successfully for a range of high-value assets (e.g. real estate, cars, fine art). Identification presented is that of the agent or an

alias, and the paperwork is completed in the agent's or alias's name.
4. Property acquired from auctions may be sold on to uninvolved third parties and the proceeds reinvested elsewhere (layering), or returned to the original source for his or her personal enjoyment (integration).

Key facts

Auctions can be used in a variety of ways. Cash purchases can be used to place criminal cash into the system, but auctions might also be used as a vehicle for buying a lot of different high-value items and then trading them on almost immediately in exchange for clean money which can then be reinvested elsewhere.

It goes without saying that the kinds of auctions that money launderers are most likely to be interested in are the ones where high-value items such as fine art, cars, antiques or real estate (both property and land) are being offered for sale. However, auctions of lower-value goods (e.g. second-hand car auctions) can also provide a ready marketplace in which criminal gangs are able to offload stolen property in exchange for hard cash, or change criminal cash into saleable assets.

The increasing availability of online auction sites offers the added attraction in that as a relatively new phenomenon they are not as yet subject to rigorous regulation. Online auctioning also enables participants to trade in relative anonymity, and to trade virtually anything with virtually anyone without too much scrutiny.

Money launderers' perspective

The attraction of auctions from the money launderers' point of view is the option to carry out the majority of transactions without ever having to be physically present or in direct contact with the other participants.

The auction environment is one in which it is quite normal for paying participants to act via intermediaries or agents, and so the non-presence of a purchaser does not draw attention.
Another advantage of the auction environment from the launderers' point of view is that many of the transactions are 'one-offs' and not the kind of relationship transactions involved in many kinds of other financial business.

Possible red flags

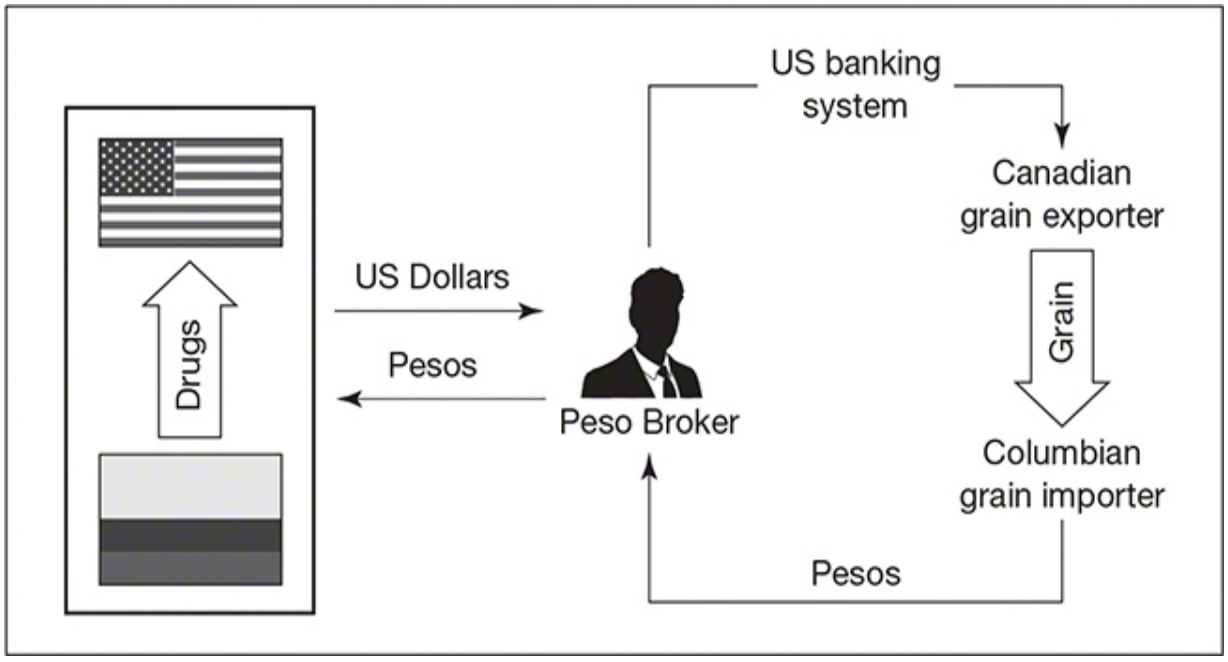
Transaction features and behaviours that might give cause for concern include the following:

- unwillingness or inability on the part of purchasers or their agents to give identification or other details
- cash settlements where cash would not normally be used as the method of settlement, particularly where the amounts involved are very large
- unusual purchasing patterns that do not appear to fit with what is known about the purchaser or their agent (e.g. purchase of a large number of high-performance cars when the purchaser does not appear to be in the car business or to have any other reason for making such a purchase, other than to use up large amounts of money)
- successful high-value bidders who are unwilling or unable to identify themselves
- third party intermediaries who are unwilling or unable to identify their clients
- cash settlement of high-value purchases, where use of cash would be unusual
- large-scale purchase of multiple items which cannot be explained and does not match the apparent business of the

purchaser (e.g. car dealership, property developer).

Black market peso exchange

Black market peso exchange



Source: © Lessons Learned Ltd 2019

How it works

This example is based on a real case.

1. A Colombian drug cartel imports and sells drugs in the US for US dollars cash.
2. The cartel then sells the US dollars to a peso broker for Colombian pesos, which are banked by the cartel in Colombia.
3. The peso broker pays the US dollars into US bank accounts he controls using ‘smurfs’.
4. He then uses the funds to pay a Canadian company to ship grain to - Colombia (on behalf of a Colombian import company).
5. The Colombian grain importer sells the grain in Colombia for pesos and repays the broker in pesos, thus replenishing the broker’s supply of

Colombian currency.

6. The cartel has no involvement beyond the initial shipping and sale of drugs and the sale of the criminal proceeds to the peso broker. The rest of the activity is carried out independently of the cartel.

Key facts

The term ‘black market peso exchange’ has its origins in the 1980s when the Colombian drug cartels dominated the illegal drugs trade in the US. Black market peso exchange was the system developed by these cartels to repatriate profits from drug sales in the US. The system has been adopted by criminal organisations in other parts of the world and the term ‘black market peso exchange’ is now applied more generally to the same system of money laundering, wherever it is used.

The system requires the collusion of an importer. It is made attractive to importers by providing them with the currency they need at a better rate of exchange than would normally be provided by local banks.

Money launderers’ perspective

From the money launderers’ point of view the system has a number of attractions. For one thing, the favourable exchange rate means that launderers may not have difficulty in finding an unscrupulous importer willing to collude with them. Also, the way in which this collusion works means that the launderers can do away with techniques such as over-invoicing or under-shipping in order for the colluding party to make a profit, since the profit can be made legitimately when the goods are sold on at their final destination. Since fraudulent tactics such as over-invoicing are not required, the goods and their value can be presented to customs exactly as they are and, since no other crime has been committed, there is a greatly reduced risk that the authorities’ attention will be alerted.

Another great advantage for the launderers is that, once the initial risky enterprise of importing and selling drugs has been completed and the cash proceeds offloaded via a peso broker, the connection between the money and the criminal activity that produced it is virtually broken. The cartel has no involvement beyond its initial dealings with the peso broker, and so the risk of exposure is greatly reduced.

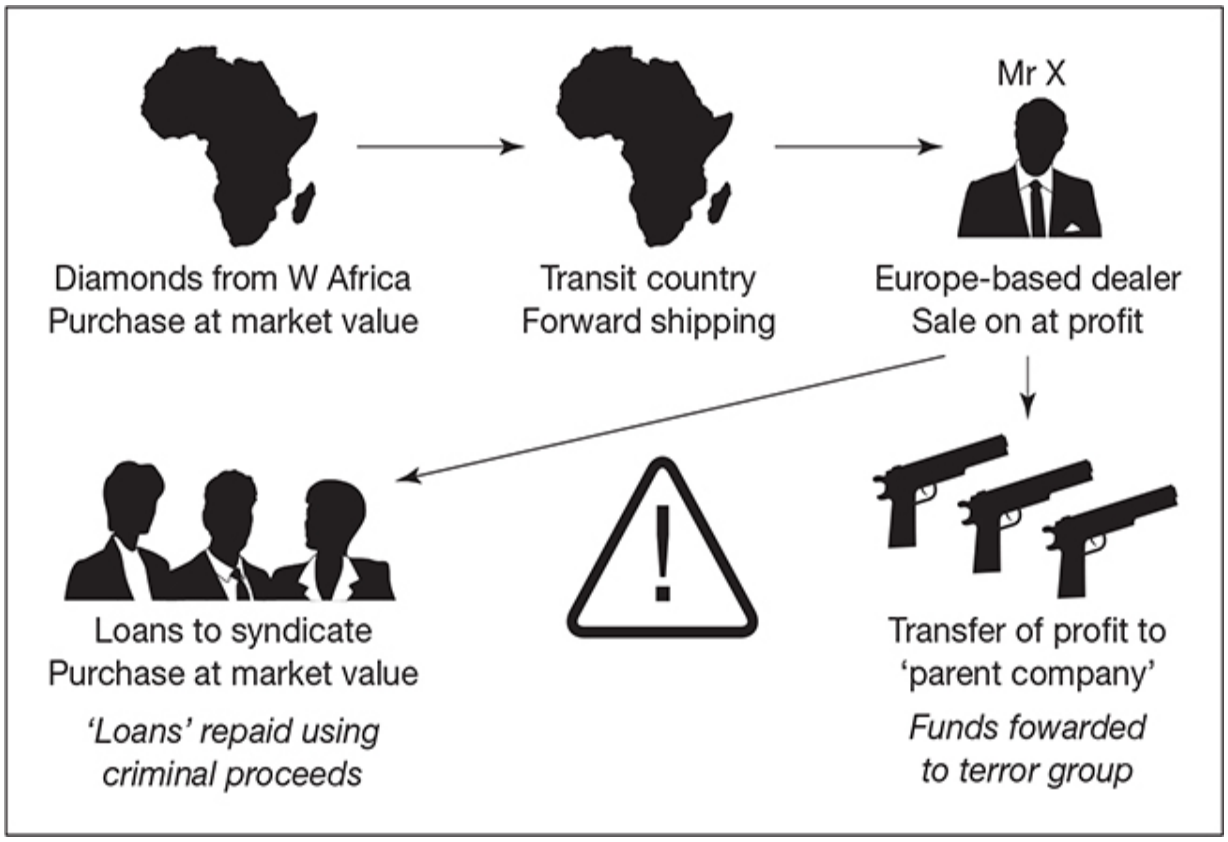
Possible red flags

These are:

- any ‘money brokering’ business that deals in cash exchanges of currencies commonly associated with this type of exchange system
- frequent cash deposits just below the local cash transaction reporting threshold (where one exists)
- a regular financial relationship with an import/export business where such a relationship does not fit what is known about the customer
- revenue streams do not make sense, given what is known about the entities involved and their normal business activities.

‘Blood’ diamonds

Blood diamonds



Source: © Lessons Learned Ltd 2019

Use of 'blood' diamonds in relation to criminal funds

This example is based on a real case.

1. 'Blood' diamonds were purchased at the local market value in Western Africa and shipped through another country, arriving eventually with a Europe-based diamond dealer, for sale on to other customers at a profit.
2. Among the various customers purchasing these diamonds were members of another diamond dealing family who were also involved in a number of criminal activities including illegal diamond trafficking. They raised loans which were used to purchase diamonds from the dealer. The terms of these loans were such that they were able to repay them quickly, using criminal funds. In other words, the legitimate loan funds were exchanged for diamonds and then replaced with criminal funds.
3. The diamonds could then be sold on legitimately at a profit.

4. While using the sale of diamonds to help these criminals to launder their funds, the dealer was also using the profits from other sales to help fund terrorism.
5. Profits from sales were transferred on to an intermediary entity, before being passed finally to Al-Qaeda.

Key facts

Diamond production across the world is concentrated into a relatively small number of countries, including several countries in Western Africa where war and conflict have led to the breakdown of formal and legitimate controls in the diamond-producing regions. In the absence of such controls the 'warlords' and criminal gangs have taken their opportunity to move in and exploit diamond production for their own ends.

Many of the proceeds of diamond sales from these regions are used by the warlords to fund arms purchases and further conflict. It is this association between bloodshed and diamond production in the region which has given rise to the term 'blood diamonds'.

In recent years there have been increasing concerns that terror groups may also be using the market in 'blood' diamonds to fund their own activities.

Money launderers' perspective

Diamonds and other precious gems have long been used by money launderers as a means to convert criminal cash into a high-value, compact and easily tradable asset.

Their compactness and lack of weight and odour means that they can be easily concealed and are therefore easy to transport across borders.

Diamond production and diamond trading are both concentrated in a relatively small number of locations, and it is clearly in these locations or in transactions *involving* diamonds that particular vigilance for this money laundering typology is required.

As regards ‘blood’ diamonds the obvious high-risk jurisdictions are the diamond producing countries of Western Africa. High value, cross-border transactions involving these countries carry at least some risk of a link with the trade in ‘blood’ diamonds.

Possible red flags

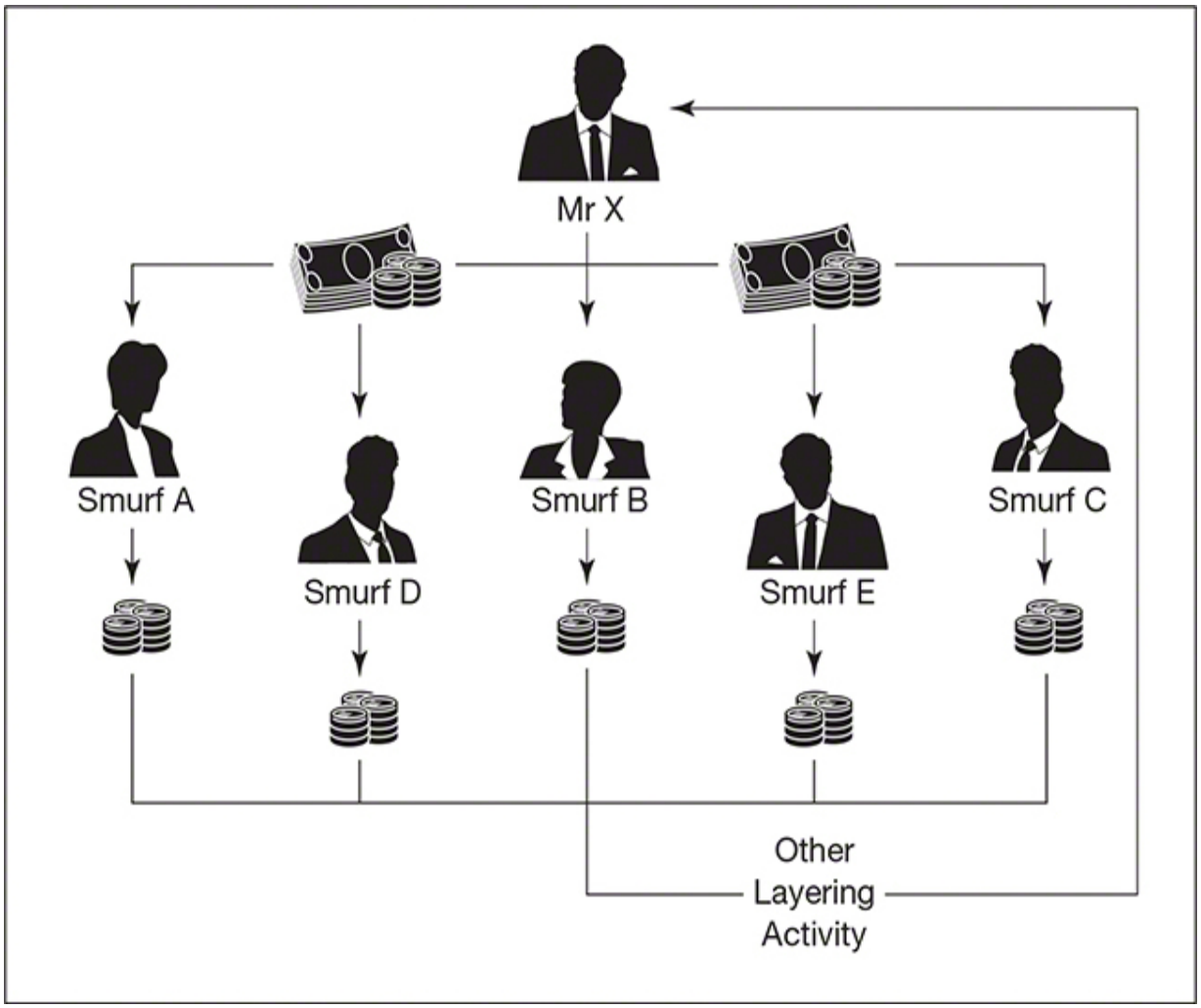
Transactions that might give cause for concern and should certainly give rise to enhanced due diligence include the following:

- transactions that have originated in or passed through countries associated with the production of ‘blood’ diamonds
- any unusual transactions involving companies active in the diamond trade
- any cash transactions (deposits or withdrawals) that can be linked to the trade in diamonds
- any transaction that can be linked to the trade in diamonds and which does not fit with the known business of the individual or entity in question
- significant unexplained deposits from companies active in the diamond trade
- large-scale, cross-border, funds transfers involving countries known to be a source of ‘blood’ diamonds
- cross-border funds transfers involving nationals/residents of diamond producing areas of Western Africa
- unexplained large international funds transfers to known diamond traders, followed by immediate withdrawal in cash
- very ‘regular’ levels of funds and cash flow in diamond trading businesses (fluctuations would be more normal)

■ any transaction with the diamond trade that cannot be explained by an individual's or company's known business.

Casinos

Casinos



Source: © Lessons Learned Ltd 2019

Casinos as a vehicle for the placement of criminal funds

1. The launderer distributes the cash proceeds of crime in relatively small amounts to a large number of 'smurfs'.

2. Each smurf exchanges cash for chips at a casino.
3. Smurfs play some of the chips but then credit the remainder to an account in their own name or some other third-party account.
4. The banked money is then reinvested elsewhere as part of the layering process before finally being returned to the criminal for his or her enjoyment.

Key facts

Casinos are primarily of use for placement activity, since they provide an environment in which cash circulates freely and in fairly large quantities. It is not, therefore, too difficult for the criminals to introduce the cash proceeds of their illegal activities into this circulation.

The placement activity occurs in the exchange of cash for gambling chips. This exchange generally takes place in a physical casino rather than an online casino environment.

However, online gambling websites offer patrons the opportunity to set up accounts where they can deposit funds and have them available for play. The same accounts can also be used by money launderers as temporary places to store money and keep it circulating gently via a bit of online gambling, before it is moved wholesale to be reinvested elsewhere.

Money launderers' perspective

From the money launderers' point of view the casino environment is uniquely suitable for placement purposes because of the large amounts of cash which are moving around and the rapid speed at which all this cash can change hands.

It is also possible from the launderers' point of view to establish a fairly large network of willing collaborators ('smurfs') who are only too happy to help process the money in exchange for some gambling 'pocket money'.

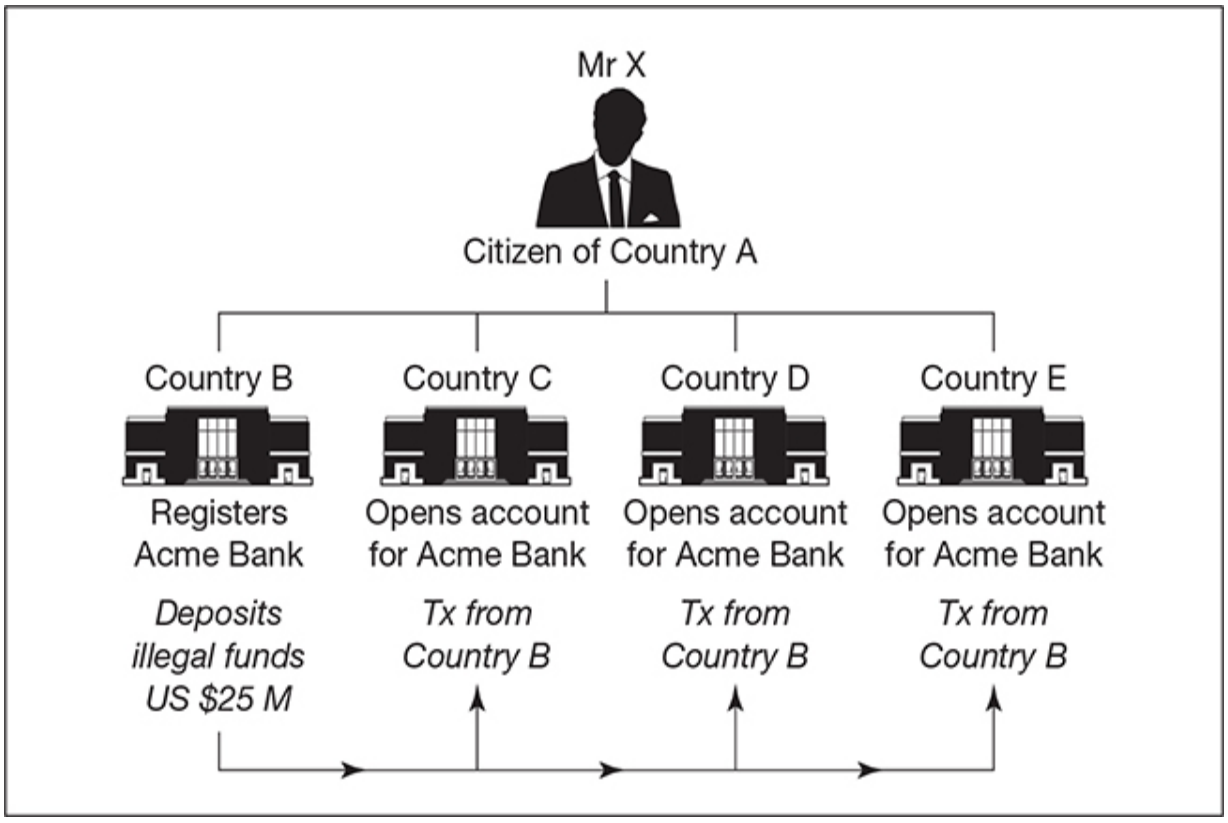
Possible red flags

Things to look out for include the following:

- patrons who are unable or unwilling to provide identification when purchasing chips or cashing chips in
- patrons whose chip purchases consistently do not match their gambling, i.e. purchases in very large quantities of which the patron then only plays a very small proportion, before cashing them all in again
- patrons whose appearance and apparent status appear inconsistent with the values of their chip purchases (may indicate that they are making the purchase on behalf of a wealthier third party)
- instructions to forward the cash-in value of leftover chips to someone other than the patron (may also indicate that they are acting as an intermediary for an unknown third party).

Correspondent banking

Correspondent banking



Source: © Lessons Learned Ltd 2019

Use of correspondent bank accounts for money laundering

This example derives from a real case. Mr X was a citizen of Country A. He registered a bank in Country B ('Acme Bank'). Acme Bank was a shell bank, had no real physical presence, no staff and no remit ever to provide services to anyone other than Mr X; in fact its sole purpose was to act as a vehicle for Mr X's criminally obtained money. Mr X deposited $25 million of his money before moving on to Country C.

In countries C, D and E Mr X went to various banking institutions and, acting as a representative for Acme Bank, established correspondent banking accounts in the bank's name. He then used the correspondent banking services of the host banks to transfer funds to Countries C, D and E from Acme Bank's accounts in Country B.

Using this network of correspondent banking accounts Mr X was able to move money across jurisdictions, from where it was used for the purchase of high-value and highly tradable goods.

Key facts

Correspondent banking relationships are effectively agreements for one bank to provide services for another in jurisdictions where the first bank does not have a physical presence. It is a customer–supplier relationship in which the 'respondent' bank is the customer and the 'correspondent' bank the one that provides the services. The relationship permits the respondent bank to move money via the correspondent bank's own accounts and thus to offer its customers a range of services in countries where it does not normally operate. There are inherent risks in the relationship, because in many of these transactions the correspondent bank does not have direct contact with the customer entity and has to rely on the efficacy of the respondent bank's customer identification and due diligence effort.

Money launderers' perspective

Weak or inadequate customer identification and due diligence procedures on the part of the respondent bank, combined with the indirectness of the relationship between the customer entity and the correspondent bank, provide increased opportunities for concealment and this of course is attractive to money launderers. The fact that the money is transferred via the respondent bank's accounts and not via personally named accounts further enables this concealment.

Money launderers might also seek to create their own 'banks' and use these to establish their own correspondent banking relationships. The banks registered by the money launderers may be 'shell banks' that exist in name only or 'pocket banks' controlled by a single individual or group. The deposits they hold are the criminal funds that the criminals are seeking to launder. These shell or pocket bank identities are then used to establish correspondent banking relationships with legitimate banks around the world. The relationship enables the money launderers to move their criminal funds from the shell banks' accounts, via the legitimate banks' own accounts, to new destinations in other countries and other banks.

Possible red flags

There are two specific problems to look out for:

1. potential flaws or weaknesses in a respondent bank's own AML - standards and procedures
2. use of shell bank structures to establish correspondent banking - relationships for the sole purpose of laundering money.

With regard to potential problems in the AML and due diligence carried out by the respondent bank, 'red flag' issues include:

- a lack of background knowledge about the bank's customers
- absence of originator or beneficiary information for transfers passing through the bank
- slackness with regard to the entities to whom the bank provides its own correspondent banking services.

With regard to the possible use of shell bank structures in relation to correspondent banking, 'red flag' issues include any problems in identifying the owners of the bank or its location, or in obtaining evidence of its normal operating activities.

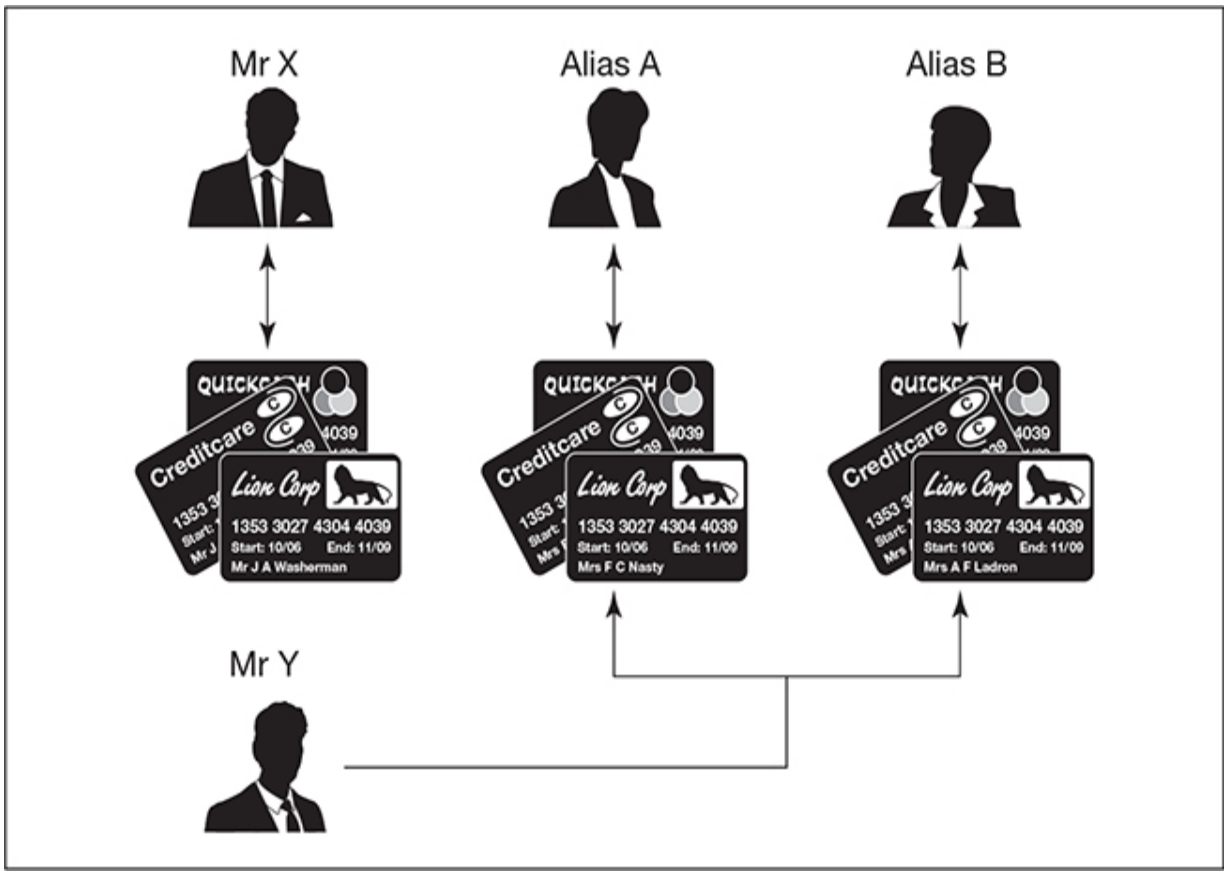
It is also possible that a legitimate bank may unknowingly use its own correspondent banking relationship to transfer via the correspondent bank's accounts criminal funds that it has failed to identify. Tell-tale signs that a bank's relationship with another bank might be being used in this way include:

- numerous requests for large volume wire transfers
- unusually frequent and repetitive transactions

- transfers whose destination do not conform with the respondent bank's normal business activities
- the respondent bank's ownership structure cannot be verified
- the respondent bank has no real physical presence
- the respondent bank is unable to provide background detail regarding entities for whom it has requested services
- the respondent bank is unable to provide originator details for transfers for which it is an intermediate bank
- the respondent bank provides correspondent banking services for shell banks
- the respondent bank permits third parties direct access to its accounts for 'payable through' transactions
- when the direction of transfer does not appear to fit with normal or expected business activity.

Credit cards

Credit Cards



Source: © Lessons Learned Ltd 2019

Use of credit cards for money laundering

This example derives from a real case.

1. A single individual (Mr X) fraudulently obtains a number of credit cards from different institutions, using a variety of different names and aliases. In some cases he holds several different cards with the same institution.
2. Using the same method of aliases he establishes further credit card accounts overseas.
3. He then uses the credit cards to make some fairly ordinary purchases (e.g. restaurant meals) and some very expensive purchases (e.g. cars, paintings, expensive jewellery).
4. He uses criminal funds to pay off the credit card debts incurred. Some of the payments are made by cheque from accounts in the name of the given card holder. Some are made by an apparently unconnected third party, Mr Y.

5. The valuable assets purchased in this way are subsequently sold on to other uninvolved parties and the proceeds of the sales are invested elsewhere.
6. The ordinary card purchases are simply used as a guise to give the impression of 'normal' daily usage of the cards.

Key facts

Credit cards are widely used in most of the world's economies and generate billions of transactions worldwide each year. No one really knows the full extent to which they are used for money laundering purposes, but there is a consensus view that they are not likely to be used at the placement stage (where criminal cash is first introduced into the financial system), and are much more likely to have a role in layering and integration activities.

Money laundering using credit cards will also tend to go hand-in-hand with other credit card-related crimes, for example, theft, where an innocent third party's identity is taken from a stolen credit card and used to establish new card accounts, and credit card fraud, where such falsely obtained cards are used to purchase goods fraudulently.

Credit cards are in such prevalence and are so widely used that *all* financial institutions across the world are potentially affected by credit card crimes.

Money launderers' perspective

One of the great benefits of credit cards for legitimate card holders is the ability, via ATM machines, to be able to access money from just about any financial institution, anywhere in the world. This benefit is clearly also advantageous to money launderers, since it gives them a means by which they can, very quickly and simply, move quite large amounts of money across international borders, without ever having to come face-to-face with a member of staff from the institution in question.

The remoteness of many credit card transactions (transactions over the telephone, over the internet, etc.) also assists money launderers in concealing their identities.
Finally, credit cards can be used to buy just about anything, with the credit card account being paid off regularly. This helps money launderers in converting their criminal funds into legitimate and saleable assets that can be sold on as part of the layering process.

Possible red flags

Transactions that might give cause for concern include the following:

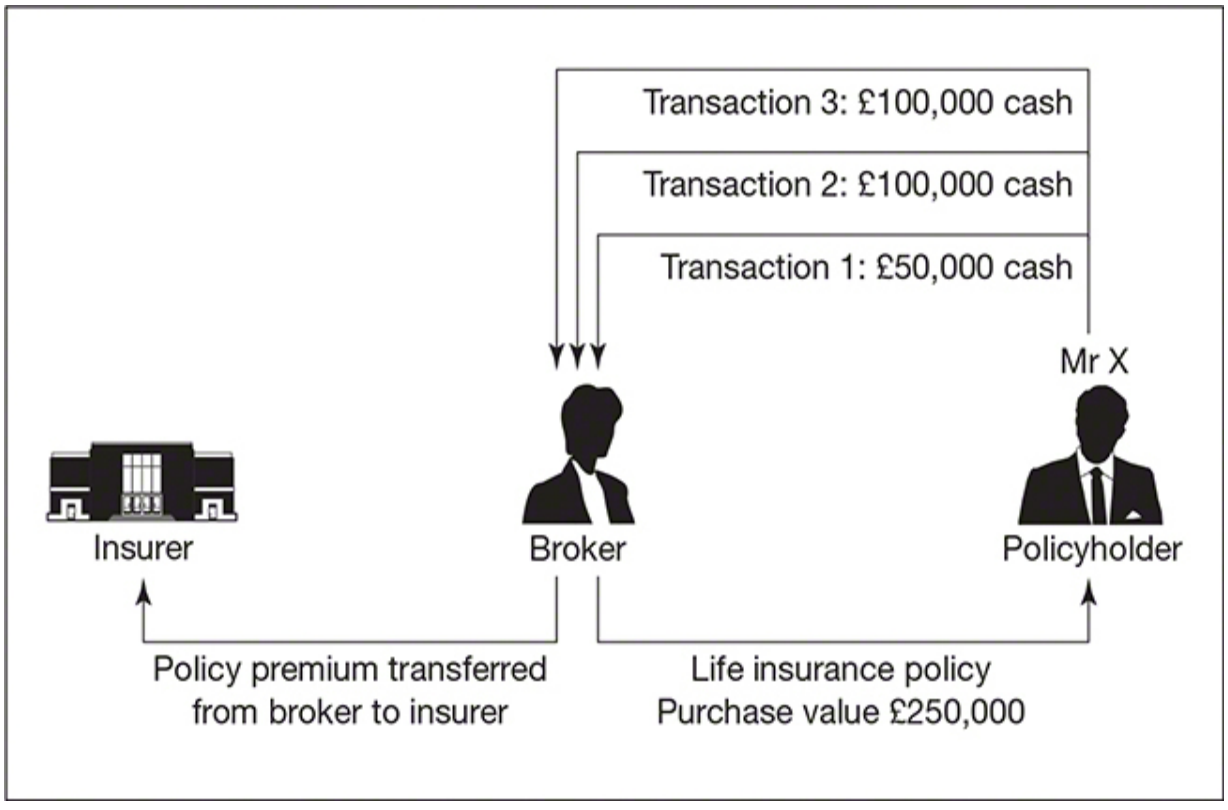
- A sudden change in the transaction patterns on a credit card account, or transactions that do not fit with the known business of the named card holder (this may indicate that the card has been stolen, or that the card account has been accessed and is being used by an unauthorised third party).
- Multiple cards in different names linked to a single residential address and/or third party settlor (this may indicate that multiple identities and different aliases are being used by a single individual).
- Third party settlement of credit card accounts (this might indicate the use of aliases as described above; or it may indicate that the card holder is in fact using the card to make purchases/launder money on behalf of an unknown third party).
- Unusually large cash settlement of credit card accounts (people *do* sometimes settle their accounts in cash, but rarely for large amounts; very large cash settlements might however be used as a means to start clearing criminal cash through the financial system).
- Unusually large and frequent cash withdrawals from offshore credit card accounts (this use of credit cards may indicate an

attempt to ‘layer’ criminal money by moving it between jurisdictions).

The terrorists involved in the 9/11 attacks used credit cards via the ATM system to withdraw money from offshore credit card accounts. Funds were paid into these accounts by third parties overseas. The terrorists drew on the funds to pay for their day-to-day living expenses, and the costs incurred in setting up their terror attacks.

Insurance

Insurance



Source: © Lessons Learned Ltd 2019

Use of insurance policies for money laundering

This example is derived from a real case.

1. The customer purchased a life insurance policy from a broker, for £250,000.
2. The £250,000 purchase price was paid in three cash lump transactions of £50,000, £100,000 and £100,000. The broker accepted these cash payments and banked them, apparently without question.
3. The broker then paid the policy premium to an insurance company, who then activated the policy on behalf of the customer.
4. The insurance company had no reason to know that the policy had been paid for by the policyholder via three suspiciously large cash transactions. They trusted the broker to have carried out adequate due diligence.

The intermediary relationship shown in this example and the heavy reliance of insurance providers on the integrity and competence of the brokers who broke their business is typical of many insurance transactions and is one of the insurance industry's greatest vulnerabilities.

Key facts

The industry is one that is particularly vulnerable because of the nature of the products it sells and the way in which those products are sold.

The products themselves are insurance policies – life, general, etc. The beneficiaries of these policies are sometimes someone different from the named policyholder. The benefit of policies can also, quite normally, be transferred from one beneficiary to another (e.g. when the primary beneficiary of a life policy dies the benefit passes to the next named beneficiary, and so on). The fact that the beneficiaries to a policy can be so readily changed makes it easier for launderers to transfer the benefit of policies, and this makes them attractive as instruments for money laundering where they have a surrender value.

The method of sale is also helpful from the money laundering point of view, because the heavy reliance on intermediaries and agents means that

launderers may never need to present personally to the company that insures them. All they need to do is find themselves an unscrupulous or unsuspecting and careless agent who is prepared to transact business without asking too many questions.

Money launderers tend to exploit insurance products using a number of basic techniques:

- placing criminal cash in the financial system by using the cash to purchase the product
- overpaying premiums and then claiming back the overpayment from the insurer
- taking out fixed term policies which are then cancelled or redeemed (the launderer pays a penalty, but the money returned is now 'clean')
- paying a heavy insurance premium and then redeeming the money indirectly, via a number of false insurance claims paid by the insurer.

Money launderers' perspective

From the money launderers' point of view the common use of intermediaries and brokers in the industry greatly assists them in concealing the identities of the named policyholders and/or beneficiaries to policies. While the insurance companies themselves might insist on rigorous due diligence they have to trust the brokers to do what is required, and if the broker does not do this the company is at risk of being used for money laundering.

Furthermore, the insurance companies that provide the policies will obviously pay the proceeds of those policies into their own bank accounts. The account holding bank is very unlikely to question the origin of the funds paid in, since the funds are paid in under the insurer's name and the bank will assume that the funds are from a legitimate source.

Another benefit from the launderers' point of view is that insurance products can *generate* money as well as laundering it. False claims on an

insurance policy give additional (criminal) revenues and income earning policies accrue value, so the launderers earn legitimate-appearing income from their insurance investments at the same time as they are using these products to launder the proceeds of crime.
Finally, the relative ease with which products can be transferred between beneficiaries is obviously advantageous in that it can be used to disguise the legal and beneficial ownership of any funds that the policy may pay out.

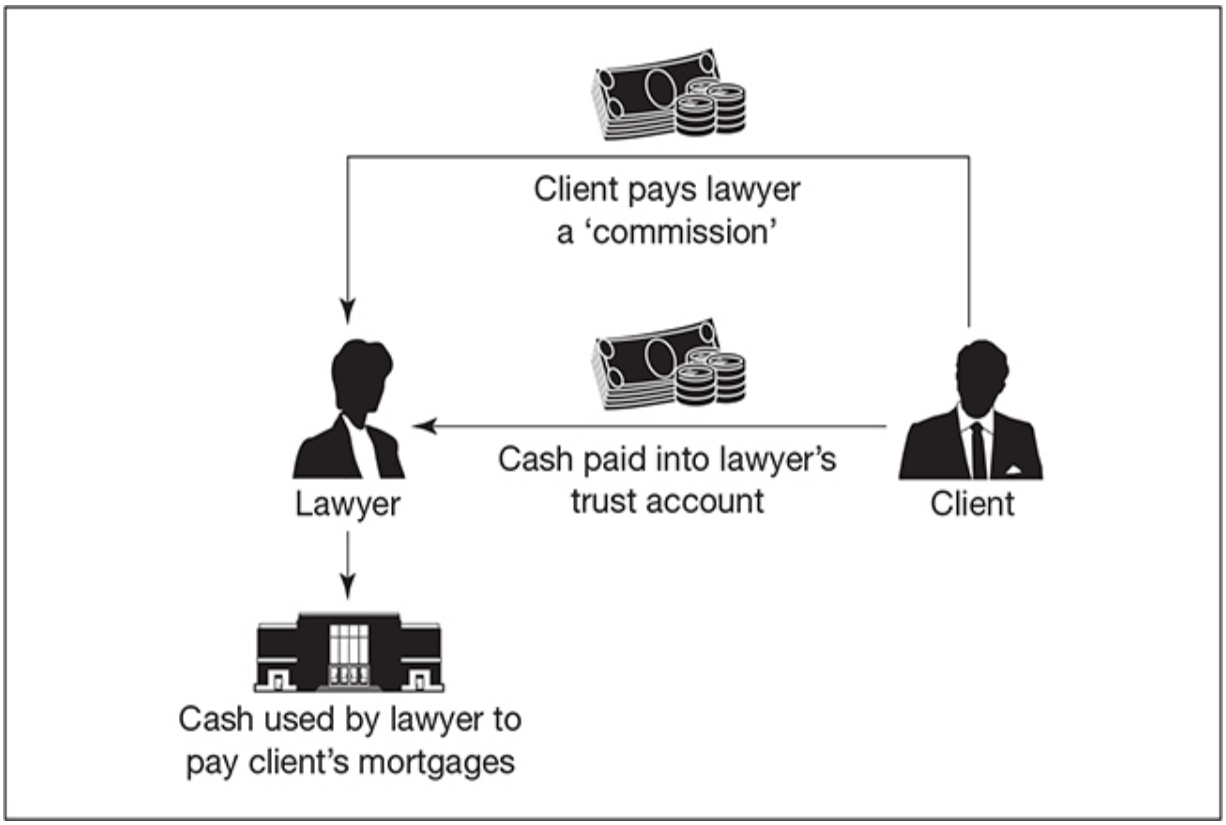
Possible red flags

Transaction features and behaviours that could give cause for concern in relation to insurance products include the following:

- pre-signed policy application forms
- purchase of products which do not make economic sense or do not fit the policyholder's apparent business needs
- payment for products via unrelated third parties
- payment for products using large amounts of cash
- unusual overpayments of premiums followed by a request to return overpaid amounts
- early redemption of policies which cannot be satisfactorily explained
- change of beneficiaries which cannot be satisfactorily explained
- unusual and frequent claims on policies, especially when payout is made to an unconnected third party.

Mortgages

Mortgages



Source: © Lessons Learned Ltd 2019

Mortgages as a vehicle for money laundering

This example is based on a real case.

1. A lawyer was instructed by his client, a drug trafficker, to deposit cash into the lawyer's trust account and then make routine payments to mortgages on properties beneficially owned by the drug trafficker.
2. The lawyer received commissions from the sale of these properties and for his services in brokering the mortgages.

Key facts

Any type of loan provides money launderers with an opportunity to acquire clean funds via the legitimate means of a loan application, and then to replace these funds in the form of loan repayments with dirty funds from

their criminal activities. A mortgage is just another type of loan that can be used in exactly this way by launderers.

However, mortgages have an added attraction in that they can be raised for very substantial amounts of money (assuming the mortgagor is able to demonstrate their ability to repay), and so they are particularly useful for the wholesale clearance of large amounts of criminal funds.

All types of mortgage are vulnerable. Launderers might use the vehicle of a property management company to purchase and develop property as part of a real business enterprise. The developed property can be sold on at a profit or rented out via letting agents. The real estate in question might be domestic *or* commercial, it does not really matter; the main thing from the money launderers' point of view is that the property is valuable and that they can raise a large mortgage on it.

The mortgage is operated as expected for a period of time, with the agreed payment instalments being made regularly and on time. Then suddenly large overpayments are made, using large amounts of criminal money wired in from accounts elsewhere, or even sometimes paid over in cash. The mortgage is fully paid off well within the agreed loan term and using criminal funds. The property, now debt-free, constitutes a significant asset which the criminal can now sell on to another third party, often at a substantial profit.

Money launderers' perspective

Mortgages are an attractive form of loan because they are linked to real estate and real estate is often a good investment that gives a good return. In other words, the launderers can build a legitimately profitable business out of their property portfolio.

Also, if the launderers are operating mortgages for different properties via a property management company, then that same company structure might also be used as a vehicle for other types of trade-based money laundering,

for example over- and under-invoicing practices involving contractors hired to do work on the properties.

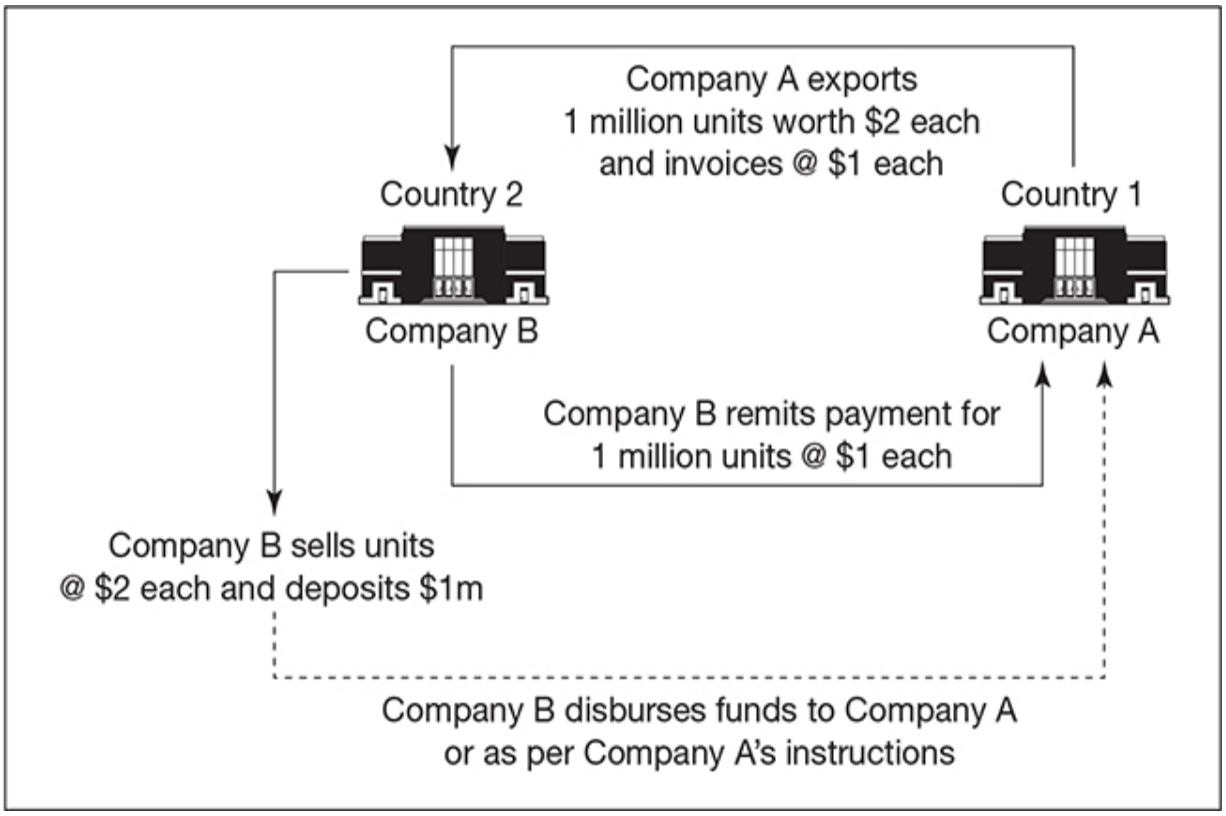
Possible red flags

Transactions and behaviours that should give cause for concern include the following:

- difficulties at application in securing identification and background details for the mortgagor
- payments from apparently unconnected third parties
- overpayments which are inconsistent with the known wealth and business of the mortgagor
- large cash payments used to reduce the amount of a mortgage
- early and unexplained repayment of a mortgage in full.

Trade finance

Trade finance


Company A exports
1 million units worth $2 each
and invoices @ $1 each
Country 2
Country 1
Company B
Company A
Company B remits payment for
1 million units @ $1 each
Company B sells units
@ $2 each and deposits $1m
Company B disburses funds to Company A
or as per Company A's instructions

Source: © Lessons Learned Ltd 2019

Trade-based money laundering via under-invoicing

1. Company A exports to Company B 1 million units of a product, each of which has a fair market value of $2.
2. Company A invoices Company B for only half the fair market value of the products supplied. Company B pays the invoice, wiring $1 million to Company A.
3. Company B then sells the products at their true market value of $2, making a $1 million profit.
4. The $1 million in profit is deposited by Company B and later disbursed according to Company A's instructions (with Company B being paid a 'consideration' in return for its services).

Key facts

Trade-based money laundering is a generic term used to describe a range of different laundering techniques using trade transactions.
The basic techniques are as follows:

- over- and under-invoicing: where there are discrepancies between the value invoiced and the value of the actual goods received
- multiple invoicing: where a product or service is supplied once but several invoices are generated (this has the same overall effect as over-invoicing)
- over- and under-shipment of goods: where there are discrepancies between the goods as described and the actual goods themselves (e.g. goods described as low-value high street clothing items but are actually high-value designer brands) – this has the same overall effect as over- and under-invoicing
- falsely described goods and services: for example, where a printing company submits an invoice for services which have never in fact been requested or provided and which are then 'paid for' using criminal proceeds.

With an increasingly global economy the opportunities for money launderers to exploit trade transactions for money laundering purposes (particularly in relation to import–export business) are also increasing.

Money launderers' perspective

From the money launderers' point of view the advantages of trade transactions are that they are so numerous. A single business can perform hundreds of transactions every day. It is relatively easy therefore to disguise a few spurious transactions in amongst all the legitimate ones. The complexity of international and foreign exchange financing arrangements can also help to obfuscate what is really going on. Illicit funds can also be commingled, concealed and transmitted alongside legitimate funds. This is

particularly true where a genuine import–export business has been co-opted into the laundering arrangements.

Possible red flags

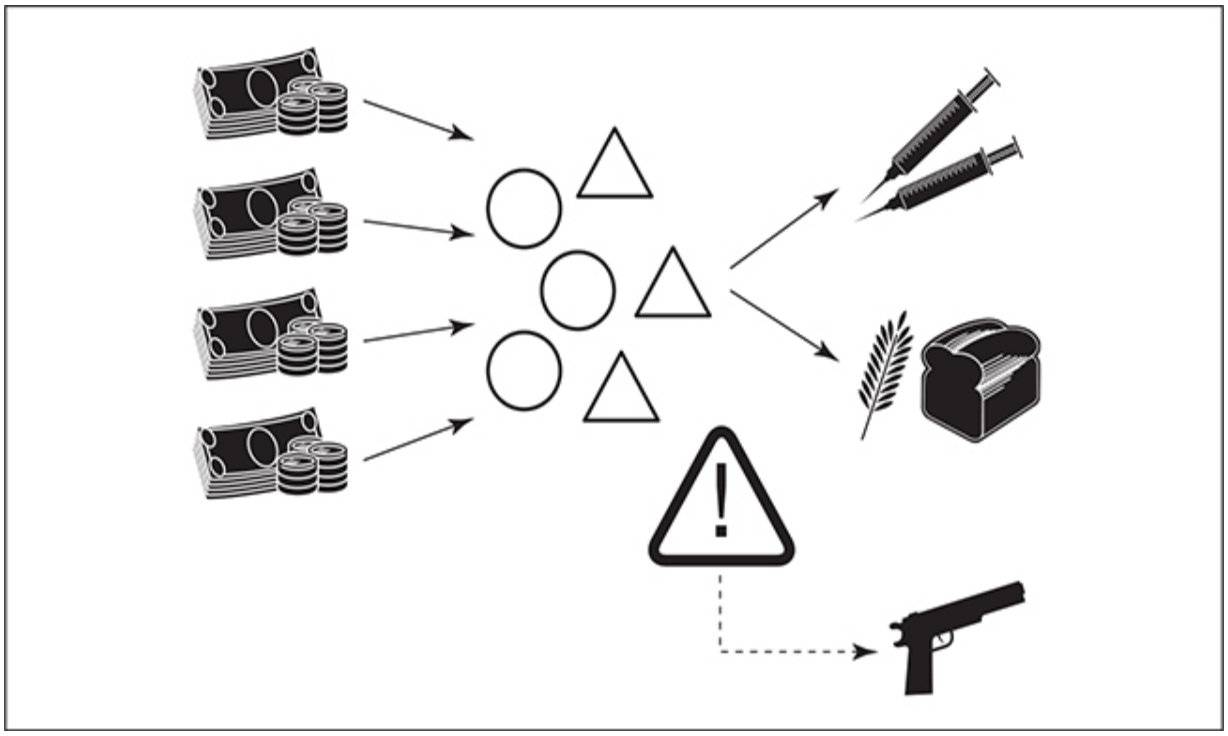
There are a number of suspicion indicators that should give cause for concern in relation to trade activities. A number of these indicators are listed below.

- the bill of lading description of goods does not match those on the invoice
- goods described do not match the actual goods shipped
- the invoiced value of the goods/services exceeds the fair market value
- the volume/type of goods/services is inconsistent with known size/nature of the entity's regular business activities
- the business transaction does not make economic sense
- goods are shipped through one or more jurisdictions for no apparent economic reason
- repeatedly amended or frequently extended letters of credit
- cash settlement of transactions from apparently unconnected third parties
- supplier and customer relationships and transactions that do not fit with the known business of the corporate entity.

TERRORIST FINANCING TYPOLOGIES

Diversion of charitable funds

Diversion of charitable funds



Source: © Lessons Learned Ltd 2019

How it works

The concept of the ‘front company’ will be familiar to anyone who deals with the prevention of money laundering through corporate structures. In the world of terrorist financing, charitable and humanitarian organisations are particularly at risk of being targeted by terrorist financiers and used by them as ‘front’ organisations to disguise the movement of terrorist funds.

1. At the start, everything is perfectly legal. The charity is a bona fide charity, doing exactly what it says it does. It receives legitimate donations from lots of different sources, often all over the world. The money received is deposited and pooled in the charity’s bank accounts...
2. From there it is sent to fund relief projects and other charitable activities around the world. The money is sent to banking outlets in or

near the organisation's projects, from where it is withdrawn, often in cash, which is used to pay for the charity's local needs.

3. These cash withdrawals are 'hijacked' by the terrorists at the point of withdrawal, i.e. the person who goes into the bank to receive the withdrawn money is an impostor acting for the terrorist group who simply poses as a worker for the charity, takes the money and vanishes, thereby channelling the money to the terrorists.

Key facts

Why should charitable and humanitarian organisations in particular be so vulnerable to exploitation by terrorist groups? The answer is simple: terrorists are frequently at their most active in the world's relief 'hot spots', which means that relief organisations and terrorists are often active in the same geographical areas. The charities and terrorists both need to move funds to the same places, and the terrorists simply use the charities to do it for them.

The fact that these areas often operate a cash economy and that the transferred funds are received in a cash form ready to use makes it that much easier for terrorist impostors to steal and divert the funds to their own causes.

Sometimes the money is 'hijacked' before it even reaches its destination via a 'plant' within the charity – a member of staff who is a sympathiser or whose cooperation has been obtained under duress, and whose authority is used to order transfers specifically for the benefit of terrorists.

Terrorist financiers' perspective

The fact that charities may operate in the same geographical areas as terrorist groups is clearly very convenient for the terrorists, since the

charities' transactions to that area provide them with a ready-made means to move their money to where it can be used by local operatives.
By 'piggy-backing' on the charities' transactions they can shift their own terrorist funds as well as hijacking funds that were originally intended for the charities' legitimate activities. The fact that they can do all this under the cover of a third-party organisation clearly helps with the problem of disguising the true purpose of the funds and the identities of those involved.

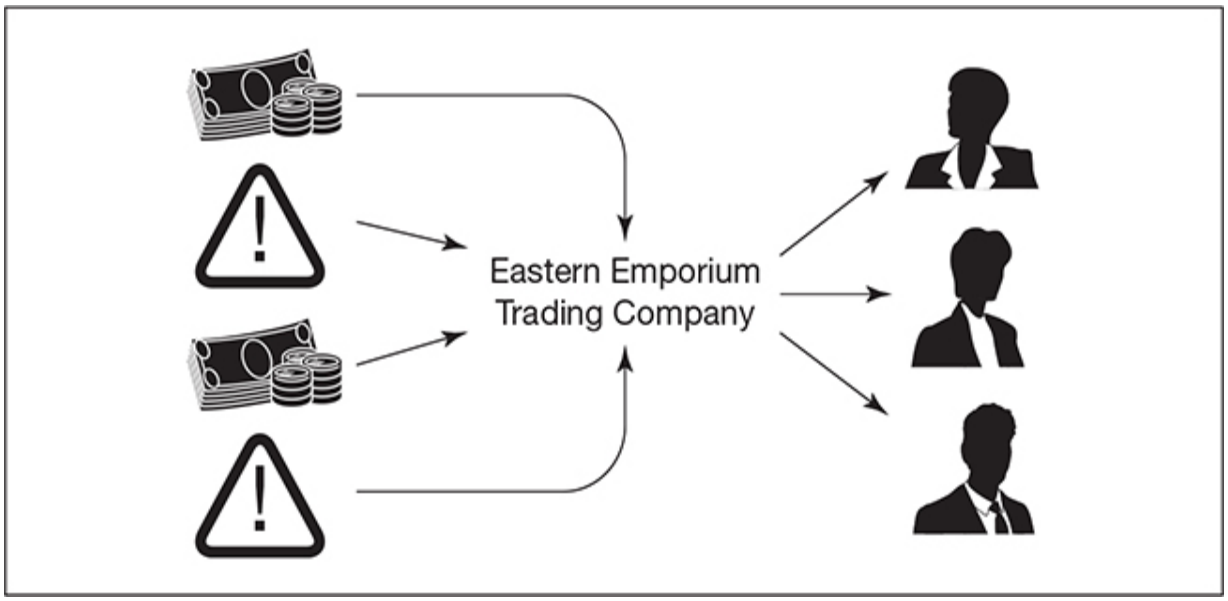
Possible red flags

These include:

- incongruities between the known sources of a charity's funding and the value of funds deposited into its account or moved through it
- mismatches between the pattern and size of financial transactions and the stated purpose and activity of the charitable organisation
- discrepancies between the known regions where the organisation is active and the destination of transferred funds
- changes in signatories that coincide with changes in the volumes and destination patterns for overseas remittances
- sudden unexplained increases in the frequency of financial transactions and the sums paid in and out of accounts.

International business transactions

International business transactions



Source: © Lessons Learned Ltd 2019

Use of business accounts

This example is based on a real case.

1. A business in a high-risk country sources and exports ethnic crafts for sale overseas. Customer businesses pay legitimate amounts of money in payment of invoices received from the business, for goods that have been supplied and purchased legitimately. The payments are often made by electronic transfer, given that the customer businesses are based overseas.
2. Alongside these legitimate revenues from its customers the business receives wired terrorist funds. These funds are commingled with the legitimate revenues in the business's accounts.
3. Individuals with signatory authority for the business's accounts then withdraw funds via local bank branches in the terrorists' target country, to fund local terrorist activities.

Key facts

Businesses that have a connection – through their ownership, their location or through their trading – with high-risk countries clearly constitute a higher-risk of involvement and may require enhanced due diligence.

Diaspora-owned businesses around the world are particularly vulnerable, since they can provide the terrorists with a ready-made network of business accounts and the assistance of the business owners of those accounts (whether willing or forced by threats of violence) can be particularly valuable.

Terrorist financiers' perspective

As indicated above, diaspora-owned businesses are potentially higher risk and may require enhanced due diligence, as the diaspora who own them (immigrants or refugees from their country of origin) may actively support the terrorists' causes in their homeland and may be quite willing to allow their businesses to be used. Alternatively there have also been cases where diaspora owners of businesses have been *forced* to cooperate with the terrorists under the threat of possible repercussions for their families, if they do not.

The network of businesses across the world – and in particular the use of import–export businesses – provides the terrorists with a network of legitimate international business via which electronic transactions may be carried out frequently, with terrorist financing transactions hidden within.

Possible red flags

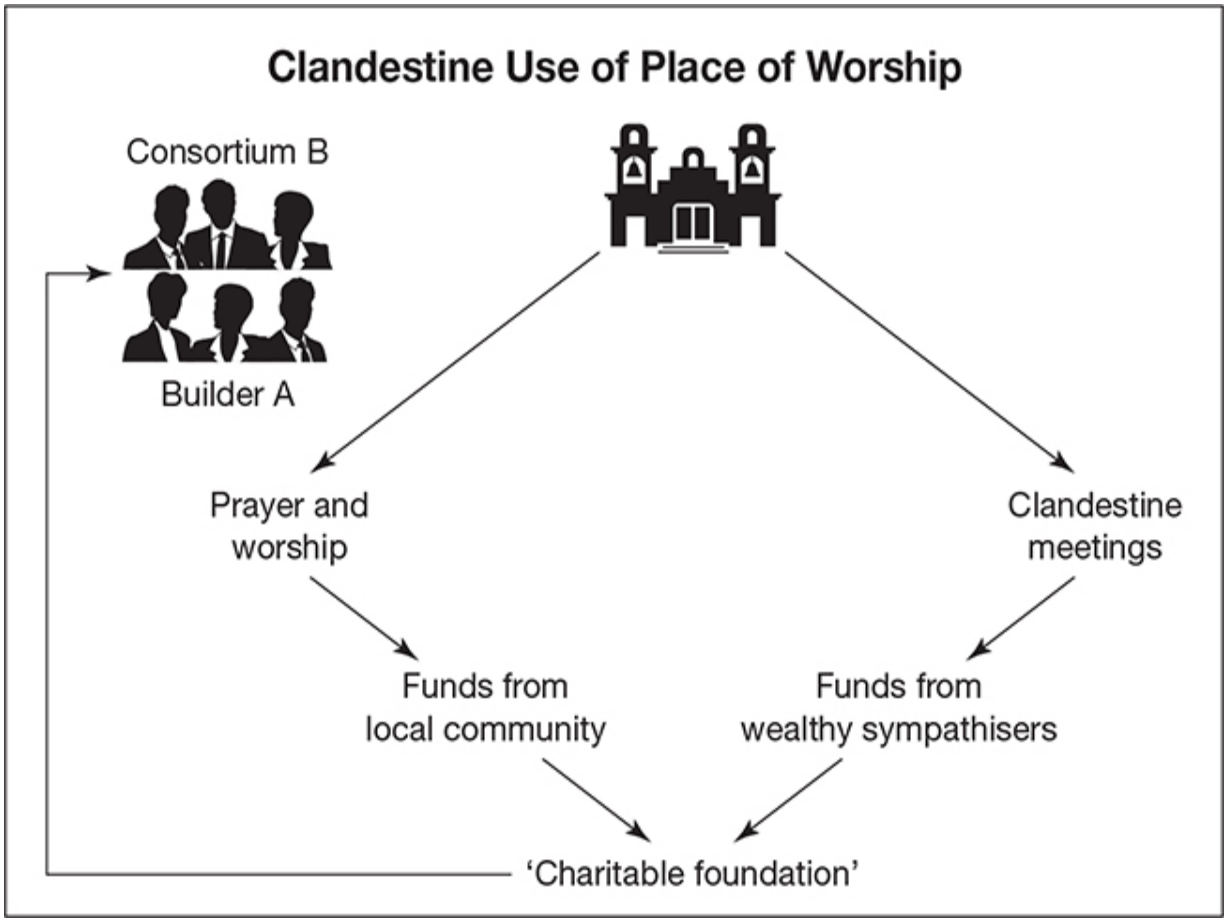
These include:

- the use of a business account to channel funds to a small number of overseas recipients, without apparent reason
- individuals and businesses in a country of specific concern who are connected by unusual or unexplained payments

- an unusually high volume of wire transfer activity into and out of a business account
- large and unusual currency withdrawals from a business account
- a business owned by nationals of countries of specific concern which undergoes a sudden and unexplained change in profile.

Places of worship

Places of worship



Source: © Lessons Learned Ltd 2019

Clandestine use of places of worship

This example is derived from a real case.

1. Builder A is the local owner of a local building company. He is also a member of a religious extremist group. He uses his company to purchase a property for renovation and sale.
2. The property is renovated and converted into a place of worship, ownership of which is then transferred from Builder A to Consortium B who are overtly a consortium of wealthy local businessmen but covertly religious extremists with links to terrorism.
3. The place of worship is opened for use. On the one hand it operates legitimately as a place for the local community to pray and worship. On the other hand it provides a convenient venue for local and visiting extremists to hold clandestine meetings.
4. Extremist meetings are used as an opportunity to raise funds from sympathisers. Legitimate donations from the local community are also collected in support of their place of worship.
5. Donations from both sources are paid into a 'charitable foundation' that determines how and where the funds will be spent.
6. The foundation is placed under the control of Consortium B, who channel funds from the foundation into terrorist causes of their choice.

Key facts

Not all terrorists are religiously motivated, and clearly it is primarily only those terror groups that have a religious fanatical agenda who are likely to make places of worship a centre for their activities.

Terrorist financiers' perspective

For religious extremist terror groups, such institutions are an obvious target as a centre for fund-raising since the people who use them for worship will be of the same religious persuasion and, even if not extreme in their views, are more likely to sympathise with some aspects of the extremists' cause and possibly to be persuaded towards supporting their ideas.

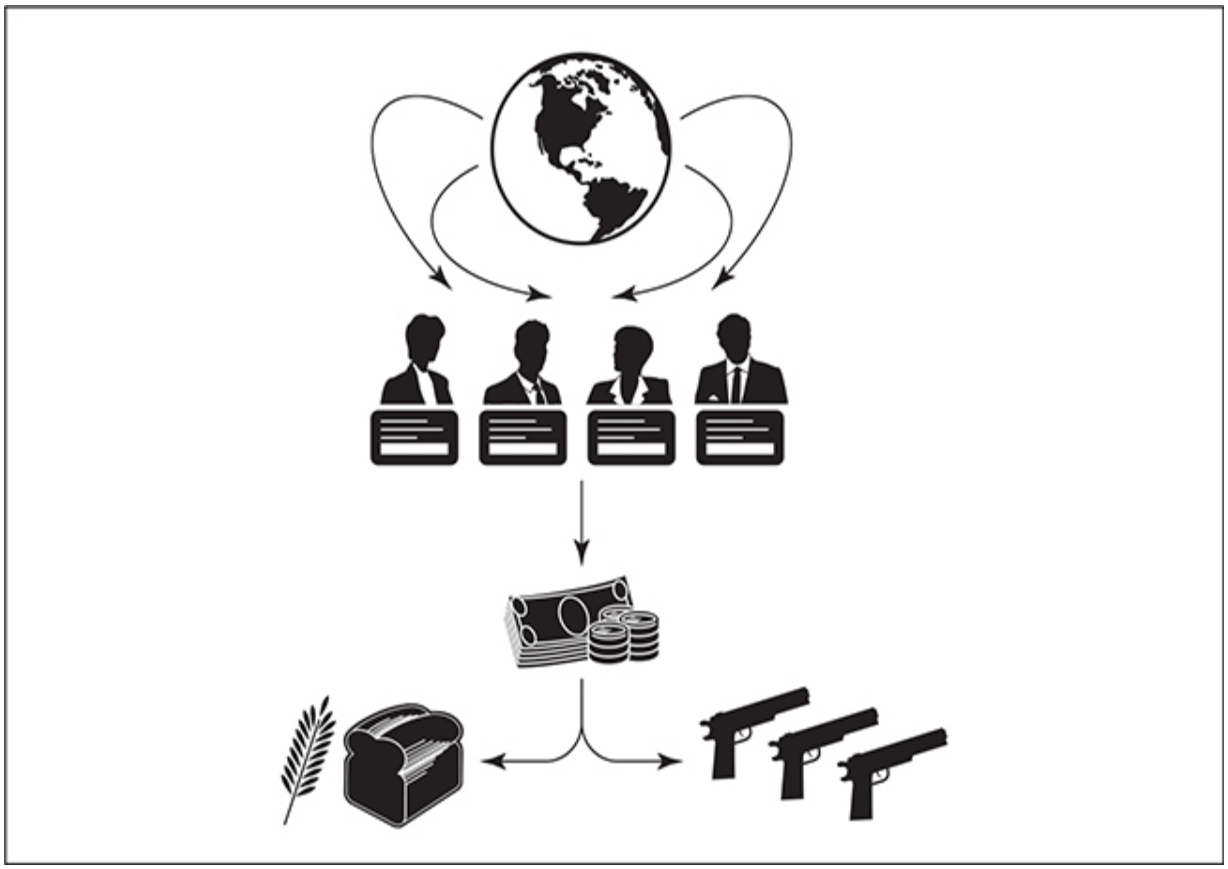
Possible red flags

These include:

- difficulties in establishing and identifying who owns and controls a centre for religious worship
- unexplained large volumes of ‘donations’ that are inconsistent with the size and wealth of the local faith community
- financial movements including forward transfers to third parties whose connection with the centre and its business are unknown or unexplained
- connections between the local faith community and countries known to be at a high risk from terrorism.

Overseas funds transfers

Overseas funds transfers



Source: © Lessons Learned Ltd 2019

How they can be used to fund terrorism

This example is based on what really happened behind 9/11.

1. Operatives used student visas or other official permissions to base themselves legitimately in the target country, where they opened bank accounts.
2. Funds were received into these accounts via electronic transfers from various overseas third-party accounts.
3. The operatives used ATM cards to make cash withdrawals.
4. They used the cash to fund their day-to-day living costs of food, rent, college fees, etc.
5. They also used the cash to fund purchases and activities in preparation for terror attacks within the host country.

Key facts

With modern technology it is a universal requirement that careful records must be kept of the originator (and now the beneficiary) details for any electronic financial transactions. This is clearly a risk to terrorists as it increases the chances of detection. However, the sheer volume of electronic transactions that are carried out globally each day acts in the terrorists' favour and reduces the likelihood that their transactions will be detected. Transactions that are unremarkable in their features are unlikely to attract the attention of banking staff or even of a bank's automated monitoring systems, and provided the terrorists keep their transactions within the bounds of what appears normal, there is a chance that they will pass unnoticed.

It is also known that the third-party originators of these overseas transfers are usually unconnected with terrorism and so would not automatically arouse suspicion when identified. The terrorist group provides the funds, but the people providing the account facilities and named as the originators of the transfers are often family members or others who are able to provide a legitimate and plausible reason for their association with the operative to whom the funds are being sent.

Terrorist financiers' perspective

Given the heightened risk of detection, why would terrorists *use* electronic transfers? One reason is the speed and immediacy of the transaction; money can be relocated and then moved electronically again and again before the authorities have even *begun* to notice anything suspicious.

Another attraction from the terrorists' point of view is the fact that electronic payment is a perfectly legal way of moving money around – unlike cash smuggling which is clearly *illegal* and a more risky method.

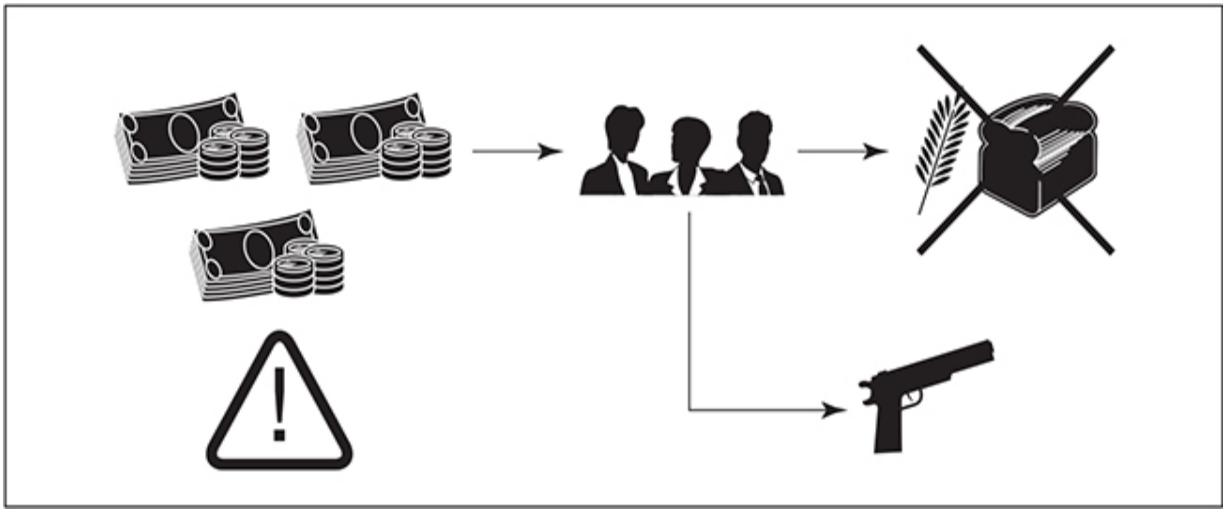
Possible red flags

These include:

- volumes of cash flowing in and out of an account that do not match the known business and resources of the account holder
- unexplained large payments from overseas accounts with no apparent reason for such payments
- account holder's transaction patterns and expenditure patterns do not match what would be expected
- transfers move to, from or through territories that are known to have a high risk of terrorist activity.

Spurious NPO networks

Spurious NPO networks



Source: © Lessons Learned Ltd 2019

Use of spurious NPOs

Charitable and humanitarian organisations provide a useful vehicle for terrorist financiers, because the operations of such organisations are often in much the same geographical area as the terrorists' own operations. Terrorist groups might infiltrate and use the banking facilities of *legitimate* charities or they might set up a few charities of their own. Here's how it works.

1. Donors pay money (often via websites) to organisations presenting themselves as not-for-profit organisations apparently engaged in 'good works' in the world's trouble spots.
2. The money is donated on the pretext that it will be used for charitable purposes.
3. But the shadowy, unseen owners and beneficiaries of these organisations are the terrorists.
4. The money is never destined for charitable works, and is diverted instead to fund terror activities.

Key facts

Spurious NPOs will operate in much the same way as shell banks, i.e. they are 'virtual' entities that have no real physical presence at any specific location. As such, most of their fund-raising will be carried out by virtual means (e.g. via the web).

The knowledge that such organisations exist does a great dis-service to legitimate, smaller and less well-known charities, since it makes people suspicious of these organisations' intentions and may make them less willing to donate funds, because of doubts about how those funds might ultimately be used.

These smaller NPOs will quite often target specific communities (e.g. immigrant populations), and the spurious NPOs run by terror groups may tend to do the same, appealing to those communities' concern for their

compatriots in their home country. Donors will often be unaware that the cause they are supporting is a terrorist cause rather than a humanitarian one.

Terrorist financiers' perspective

From the terrorist financier's point of view, the NPO is simply a useful 'front' behind which to hide their real and sinister cause of raising funds for terrorism.

Possible red flags

These include:

- difficulties in identifying the ownership structure and true owners behind the organisation
- lack of any real physical presence (e.g. a business address, land line, identifiable staff members)
- mismatches between the pattern and size of financial transactions and the stated purpose and activity of the organisation.

ACCOUNT ANALYSIS EXAMPLES

Operations, cash management and back office staff, along with managers and supervisors called upon to review accounts which have been flagged up as potentially suspicious, will need to develop a familiarity with suspicious transaction patterns, as will the compliance officers themselves. Here is a selection of accounts displaying some FATF noted patterns of potential suspicion, with explanations after each one. Soft copy versions of the accounts themselves and the explanatory notes can be requested by purchasers of this book by emailing training@lessonslearned.co.uk.

Sample Account 1

Account Holder: Mr J M Johnson					
Date	Description	Details	Receipts	Payments	Balance
30-Jan-04	Eurobank Paris	TFR		$6,750.00	$176,186.12
07-Nov-04	Eurobank Warsaw	TFR	$7,560.00		$183,746.12
15-Nov-04	Counter Deposit	Cash	$9,461.21		$193,207.33
25-Nov-04	Counter Deposit	Cash	$14,874.08		$208,081.41
28-Nov-04	University of W. America	TFR		$48,682.67	$159,398.74
12-Dec-04	Agri-Bank Kiev	TFR	$7,506.54		$166,905.28
15-Dec-04	Cash Withdrawal	ATM		$405.00	$166,500.28
22-Dec-04	ML Investments London	TFR		$71,069.27	$95,431.01
04-Jan-05	Fortuna Bank Santiago	TFR	$7,796.09		$103,227.10
08-Jan-05	Counter Deposit	Cash	$18,099.56		$121,326.66
22-Jan-05	Counter Deposit	Cash	$10,315.59		$131,642.25
31-Jan-05	Counter Deposit	Cash	$3,253.45		$134,895.70
02-Feb-05	Bonds of London	TFR		$97,966.13	$36,929.57
06-Feb-05	University of W. America	TFR		$32,677.75	$4,251.83
07-Feb-05	Counter Withdrawal	Cash		$4,251.83	$0.00
07-Feb-05	A/C Closed				

There are a number of important questions that need to be asked about this account:

- Payments to and from bank accounts in other countries: who owns the other accounts involved? What is the purpose of these transactions? What legitimate business might Mr Johnson have in France, Poland, Ukraine and Chile where the other accounts are based?
- Payments to the University of W. America: does this university exist? Why might Mr Johnson be making large, quarterly payments to this university – does one of his children study there?
- Payments to ML Investments and Bonds in London: who are these companies? Who owns them? What legitimate business do they have with Mr Johnson?

If Mr Johnson's business with these overseas recipients of his funds cannot be adequately explained, then that would be an immediate cause for suspicion.
Other indicators that might give grounds for suspicion include the following:

- the account has lain dormant for nine months, and then in the space of three months has been used to receive and transmit several sums overseas, some modest and some quite large
- at the end of a three-month period of activity the majority of the remaining funds is suddenly transferred overseas, and the outstanding balance is withdrawn in cash, before closing the account
- a large amount of cash has been paid into the account over a three-month period; where does this cash come from, and does it make sense for Mr Johnson to have this quantity of cash?

Sample Account 2

Account Holder: Mr B Harris-Beckford					
Current Account					
Date	Description	Details	Receipts	Payments	Balance
01-Jan-05	A/C Opened		$0.00	$0.00	$0.00
24-Jan-05	Radney Automotive Systems	REM	$1,611.63	$0.00	$1,611.63
25-Jan-05	Withdrawal	ATM	$0.00	$675.00	$936.63
01-Feb-05	B Harris-Beckford Loan Account 10594832	TFR	$0.00	$537.17	$399.47
12-Feb-05	Cash Withdrawal	ATM	$0.00	$337.50	$61.97
24-Feb-05	Radney Automotive Systems	REM	$1,611.63	$0.00	$1,673.60
25-Feb-05	Cash Withdrawal	ATM	$0.00	$675.00	$998.60
01-Mar-05	B Harris-Beckford Loan Account 10594832	TFR	$0.00	$537.17	$461.43
17-Mar-05	Cash Withdrawal	ATM	$0.00	$337.50	$123.93
24-Mar-05	Radney Automotive Systems	REM	$1,611.63	$0.00	$1,735.56
25-Mar-05	Cash Withdrawal	ATM	$0.00	$675.00	$1,060.56
01-Apr-05	B Harris-Beckford Loan Account 10594832	TFR	$0.00	$537.17	$523.40
15-Apr-05	Cash Withdrawal	ATM	$0.00	$337.50	$185.90
24-Apr-05	Radney Automotive Systems	REM	$1,611.63	$0.00	$1,797.53
25-Apr-05	Cash Withdrawal	ATM	$0.00	$675.00	$1,122.53
01-May-05	B Harris-Beckford Loan Account 10594832	TFR	$0.00	$537.17	$585.36
16-May-05	Cash Withdrawal	ATM	$0.00	$405.00	$180.36
24-May-05	Radney Automotive Systems	REM	$1,611.63	$0.00	$1,791.99
25-May-05	Cash Withdrawal	ATM	$0.00	$810.00	$981.99
01-Jun-05	B Harris-Beckford Loan Account 10594832	TFR	$0.00	$537.17	$444.83
Loan Account					
Date	Description	Details	Receipts	Payments	Balance

Date	Description	Details	Receipts	Payments	Balance
01-Jan-05	A/C Opened		$0.00	$23,490.00	−$23,490.00
31-Jan-05	Interest	DD	$0.00	$469.80	−$23,959.80
01-Feb-05	B Harris-Beckford Current Account 10644978	TFR	$537.17	$0.00	−$23,422.64
28-Feb-05	Interest	DD	$0.00	$468.45	−$23,891.09
01-Mar-05	B Harris-Beckford Current Account 10644978	TFR	$537.17	$0.00	−$23,353.92
31-Mar-05	Interest	DD	$0.00	$467.03	−$23,820.95
01-Apr-05	B Harris-Beckford Current Account 10644978	TFR	$537.17	$0.00	−$23,283.79
06-Apr-05	Loan Repayment	Cash	$1,822.50	$0.00	−$21,461.29
21-Apr-05	S Ericsson	TFR	$16,875.00	$0.00	−$4,586.29
30-Apr-05	Interest	DD	$0.00	$91.73	−$4,678.02
01-May-05	B Harris-Beckford Current Account 10644978	TFR	$537.17	$0.00	−$4,140.86
10-May-05	S Ericsson	TFR	$4,140.86	$0.00	$0.00

Mr Harris-Beckford appears to have a regular monthly salary of $1,611.63 and no other source of income, yet he is able to pay off a $23,490.00 loan within just a few months.

The source of the funds paid in settlement of the loan is a third party called ‘S Ericsson’ and not Mr Harris-Beckford himself. Who is this ‘S Ericsson’, and why would he or she be settling Mr Harris-Beckford’s loan for him?

Sample Account 3

Account Holder: Ms T Abrams (Student)					
Date	Description	Details	Receipts	Payments	Balance
05-Aug-04	Balance C/F				$670.77
05-Aug-04	Mercator	Card Purchase		$106.65	$564.12
12-Aug-04	Counter Deposit	Cash	$7,220.82		$7,784.94
12-Aug-04	Cash Withdrawal	ATM		$3,000.00	$4,784.94
15-Aug-04	Counter Deposit	Cash	$8,264.16		$13,049.10
14-Aug-04	American Express Card Repayment	DD		$1,487.58	$11,561.52
16-Aug-04	Cash Withdrawal	ATM		$3,000.00	$8,561.52
21-Aug-04	Visa Card Repayment	DD		$1,680.69	$6,880.83
22-Aug-04	Counter Deposit	Cash	$15,957.79		$22,838.62
23-Aug-04	Adidas	Card Purchase		$109.41	$22,729.21
25-Aug-04	Mexx	Card Purchase		$172.29	$22,556.92
26-Aug-04	Jugoexport	Card Purchase		$91.74	$22,465.18
29-Aug-04	Mango	Card Purchase		$87.09	$22,378.09
02-Sep-04	Escada	Card Purchase		$660.00	$21,718.09
07-Sep-04	Counter Deposit	Cash	$7,738.38		$29,456.47
08-Sep-04	Cash Withdrawal	ATM		$3,000.00	$26,456.47
10-Sep-04	Mercator	Card Purchase		$362.94	$26,093.53
10-Sep-04	Cash Withdrawal	ATM		$3,000.00	$23,093.53
14-Sep-04	Cash Withdrawal	ATM		$3,000.00	$20,093.53
	American Express Card			$764.55	$19,328.98

	American Express Card		$764.55	$19,328.98
14-Sep-04	Repayment	DD		
21-Sep-04	Visa Card Repayment	DD	$1,187.82	$18,141.16
22-Sep-04	Cash Withdrawal	ATM	$3,000.00	$15,141.16

Ms Abrams is a student, and most students would have very limited financial resources. However, Ms Abrams is different:

- She appears to enjoy shopping (there are a number of card purchases at department stores).
- Her credit card balances by far exceed a typical average monthly income and yet she seems able to pay these off without any problem.
- She makes large cash withdrawals ($3,000 a time).
- She seems to be getting a lot of cash from somewhere ($31,442.77 in one month alone).

How can a student afford to fund what appears to be a fairly lavish lifestyle? And where does all her cash come from? Ms Abrams' expenditure clearly does not fit the typical pattern of most students. Should you be suspicious?

This is where a knowledge of the customer and their background is so important. If Ms Abrams is known to have a rich and tolerant father who regularly gives her money and pays her debts, then the activity on her account might make sense. But if Ms Abrams does *not* have an explainable and legitimate source for her money, then there are clear grounds to be suspicious.

Sample Account 4

Account Holder: 'La Giaconda Bellisima' Italian Restaurant					
Date	Description	Details	Receipts	Payments	Balance
Thu 08-Jul	Balance C/F				$19,139.62
Fri 09-Jul	Counter Withdrawal	Cash		$2,647.75	$16,491.87
Fri 09-Jul	Counter Deposit	Cash	$3,699.88		$20,191.75
Mon 12-Jul	Counter Deposit	Cash	$7,709.84		$27,901.59
Tue 13-Jul	Counter Deposit	Cash	$3,681.18		$31,582.77
Wed 14-Jul	Counter Deposit	Cash	$4,189.99		$35,772.76
Wed 14-Jul	Naturalis Food Wholesalers	TFR		$2,439.84	$33,332.92
Thu 15-Jul	Counter Deposit	Cash	$3,654.15		$36,987.07
Fri 16-Jul	Counter Deposit	Cash	$4,141.88		$41,128.95
Fri 16-Jul	Counter Withdrawal	Cash		$2,647.75	$38,481.20
Fri 16-Jul	Porticano Vintners & Importers	TFR		$9,238.31	$29,242.89
Mon 19-Jul	Counter Deposit	Cash	$11,228.16		$40,471.05
Tue 20-Jul	Counter Deposit	Cash	$3,983.44		$44,454.49
Wed 21-Jul	Naturalis Food Wholesalers	TFR		$2,296.53	$42,157.96
Wed 21-Jul	Counter Deposit	Cash	$3,730.65		$45,888.61
Thu 22-Jul	Counter Deposit	Cash	$3,822.45		$49,711.06
Fri 23-Jul	Counter Deposit	Cash	$3,992.45		$53,703.51
Fri 23-Jul	Counter Withdrawal	Cash		$2,647.75	$51,055.76
Mon 26-Jul	Catering Supplies	TFR		$2,051.56	$49,004.20
Mon 26-Jul	Counter Deposit	Cash	$15,229.62		$64,233.82
Tue 27-Jul	Counter Deposit	Cash	$3,815.31		$68,049.13
Tue 27-Jul	Naturalis Food Wholesalers	TFR		$2,417.06	$65,632.07
Wed 28-Jul	Counter Deposit	Cash	$3,643.78		$69,275.85
Thu 29-Jul	Counter Deposit	Cash	$3,984.46		$73,260.31
Fri 30-Jul	Counter Deposit	Cash	$4,138.99		$77,399.30
[illegible]	[illegible]	[illegible]		[illegible]	[illegible]

Fri 30-Jul	Counter Withdrawal	Cash		$2,647.75	$74,751.55
Fri 30-Jul	Porticano Vintners & Importers	TFR		$9,155.69	$65,595.86
Mon 02-Aug	Rubicon	TFR		$32,938.86	$32,657.00
Mon 02-Aug	Counter Deposit	Cash	$15,027.15		$47,684.15
Tue 03-Aug	Counter Deposit	Cash	$3,643.95		$51,328.10
Wed 04-Aug	Naturalis Food Wholesalers	TFR	$0.00	$2,416.21	$48,911.89
Wed 04-Aug	Counter Deposit	Cash	$4,000.44		$52,912.33
Thu 05-Aug	Counter Deposit	Cash	$3,772.81		$56,685.14
Fri 06-Aug	Rubicon	TFR		$50,297.22	$6,387.92
Fri 06-Aug	Counter Withdrawal	Cash		$2,647.75	$3,740.17
Fri 06-Aug	Counter Deposit	Cash	$4,000.95		$7,741.12
			115,091.53		

This account demonstrates the features of a ‘front business’, i.e. an apparently legitimate business that uses its normal cash activities as a ‘cover’ for laundering criminal cash.

The restaurant’s daily cash takings average between $3,500 and $4,000. Takings for Friday and Saturday are banked together in a single deposit, every Monday. If the average daily takings are as described above, then the Monday deposits should be between $7,000 and $8,000. On Monday 12 July the restaurant deposits $7,709.84 into its account, which seems fine. However, on Monday 19 July the deposit has increased to $11,228.16. A week later, the deposit is even bigger ($15,229.62). A similar amount ($15,027.15) is deposited a week later.

The restaurant owners might argue that the increased deposits simply reflect the increasing success of their restaurant. But the daily takings throughout the rest of the week have not increased. Also, the restaurant makes regular payments to its suppliers (weekly payments to Naturalis, fortnightly payments to Porticano and monthly payments to Catering Supplies) and these do not appear to have increased to reflect any increasing throughput in restaurant trade. And although turnover has apparently doubled, the restaurant continues to pay the same in cash wages to staff ($2,647.75 per week). If the restaurant were taking more customers then you would expect

to see a corresponding increase in the restaurant's expenditure, but the payments to suppliers and staff remain constant.

What all this indicates is that the restaurant is using the cover of its takings to deposit increasing amounts of criminal cash. On Mondays the restaurant deposits its taking from both Friday and Saturday, which means that the amounts involved are larger than on other days of the week. The restaurant is hoping that the bank will not notice that these large Monday deposits are getting even larger each week.

Then, all of a sudden, the restaurant appears to experience some sort of financial crisis. Almost all the restaurant's funds are suddenly transferred in two large transactions on 2 and 6 August, to a company called 'Rubicon'.

This gradual accumulation of criminal funds under cover of an operating business, followed by the sudden transfer of the funds to a third party, is typical 'fronting' behaviour.

Note: a training film dealing with a front company can be previewed at http://www.antimoneylaunderingvideos.com/player/red_flags_aml.htm.

Sample Account 5

Account Holder: Ms G Browning					
Date	Description	Details	Receipts	Payments	Balance
21-Aug-04	A/C Opened				€0.00
24-Aug-04	Eurobank Paris Acct 30248588	REM	€25,000.00		€25,000.00
	Eurobank Dusseldorf Acct 30484858	REM	€27,750.00		€52,750.00
	B V Duran	REM	€24,300.00		€77,050.00
	Counter Deposit	CASH	€14,957.00		€92,007.00
	J Rocca	REM	€23,550.00		€115,557.00
	Agri-Bank London Acct 39575739	REM	€25,000.00		€140,557.00
	Counter Deposit	CASH	€14,890.00		€155,447.00
	R Inman	REM	€23,750.00		€179,197.00
25-Aug-04	Eurobank London Acct 23043957	REM	€27,500.00		€206,697.00
	Eurobank Madrid Acct 305848749	REM	€22,550.00		€229,247.00
	B V Duran	REM	€25,460.00		€254,707.00
	K Priss	REM	€25,870.00		€280,577.00
	Counter Deposit	CASH	€14,950.00		€295,527.00
	Agri-Bank Roma Acct 39575739	REM	€23,750.00		€319,277.00
	K Priss	REM	€25,000.00		€344,277.00
29-Aug-04	R Toledo	REM	€25,550.00		€369,827.00
	Eurobank Paris Acct 30248588	REM	€27,500.00		€397,327.00
	J Rocca	REM	€24,750.00		€422,077.00
	Counter Deposit	CASH	€14,989.00		€437,066.00
	B V Duran	REM	€26,700.00		€463,766.00
	Agri-Bank London Acct		€27,000.00		€490,766.00

	Agri-Bank London Acct 39575739	REM	€27,000.00		€490,700.00
	R Inman	REM	€24,500.00		€515,266.00
30-Aug-04	F W Professional Services	TFR		€375,000.00	€140,266.00
04-Sep-04	F W Professional Services	TFR		€125,000.00	€15,266.00

This account demonstrates several features consistent with it being used as a conduit for criminal funds and cash, which are then transferred on to other accounts for further laundering.

Ms Browning's account shows several receipts each day, from a variety of different sources. These receipts include a large number of transfers from other bank accounts, all between €20,000 and €30,000 in size. These are not insubstantial transfers. They were made via banks all over Europe, and by a large number of different originators. This is not a normal banking pattern for most people and would, in most cases, give immediate grounds for suspicion.

Ms Browning's account also shows a number of cash deposits at just under €15,000 indicating that she is possibly aware that cash transactions of more than €15,000 are likely to be subjected to intensified transaction surveillance. It is notable that the cash transactions shown here all fall below the €15,000 threshold, thereby avoiding the additional scrutiny that they might otherwise attract. This pattern of transactions is typical of 'smurfing' behaviour.

After several days during which money is deposited into the account, Ms Browning suddenly transfers most of the money out again. The money is transferred in two instalments to a single beneficiary, identified as 'F W Professional Services'.

This account profile should give rise to at least two key questions:

1. Who are the depositors of funds, and what business do they have with Ms Browning?
2. What kind of business is 'F W Professional Services', and who are the beneficial owners behind it?

Sample Account 6

Account Holder: The Enlightenment Trust – Raising Awareness of Poverty – Euro Account					
Date	Description	Details	Receipts	Payments	Balance
01-Feb	A/C Opened				€0.00
01-Feb	Opening Deposit	TFR	€1,800,000.00		€1,800,000.00
28-Apr	Interest		€9,000.00		€1,809,000.00
28-Apr	Petrolisum 2 Account	TFR	€525,000.00		€2,334,000.00
28-Jul	Interest		€11,670.00		€2,345,670.00
28-Oct	Interest		€11,728.35		€2,357,398.35
28-Jan	Interest		€11,786.99		€2,369,185.34
05-Feb	Santo Rico Investments	TFR		€2,369,185.34	€0.00
05-Feb	A/C Closed				

This account has been opened and has then laid virtually dormant for a whole year, accumulating interest on its deposits. At the end of the year, the total funds in the account are suddenly and inexplicably remitted to a third party called 'Santo Rico Investments'. The account is then closed.
This is just one of several transaction patterns that has been identified as potentially suspicious by the Financial Action Task Force:

- account is opened
- account lays dormant
- large transactions are affected
- account is closed or rendered inactive again.

Key questions to ask about this account might include the following:

- What is the source of the initial opening deposit?
- Who are the 'Enlightenment Trust' and what do they do?
- Does the amount of money involved fit the known business of the 'Enlightenment Trust'?
- Who are 'Santo Rico Investments' and what is their involvement with the 'Enlightenment Trust'?

Remember that people involved in the financing of terrorism have sometimes deliberately chosen account names to give the impression that the funds belong to an organisation with charitable status. Such accounts

can receive or handle ‘donations’ from a wide number of ‘donors’ without appearing unusual or suspicious. It is important to ‘know your customer’ and to be as sure as you can be that their stated business purpose is legitimate, and not just a ‘cover’ for something more sinister.

Sample Account 7

Account Name: Janus Investments					
Date	Description	Details	Receipts	Payments	Balance
22-Jan-11	A/C Opened				$0.00
22-Jan-11	Opening Deposit	Cheque	$111,475.00		$111,475.00
26-Feb-11	Janus Holdings Boston	TFR		$55,400.00	$56,075.00
28-Feb-11	Janus Investments Dubai	TFR		$56,075.00	$0.00
28-Feb-11	A/C Closed				

Account Holding Branch: Boston MASS					
Account Name: Janus Holdings					
Date	Description	Details			Balance
01-Feb-11	A/C Opened				$0.00
01-Feb-11	Opening Deposit	Cheque	$110,057.50		$110,057.50
03-Feb-11	Counter Deposit	Cheque	$51,648.46		$161,705.96
26-Feb-11	Janus Investments Boston	TFR	$55,400.00		$217,105.96
01-Mar-11	Janus Investments Dubai	TFR	$50,000.00		$267,105.56
03-Mar-11	Counter Withdrawal	Cash		$9,500.00	$257,605.56

Account Holding Branch: Dubai					
Account Name: Janus Investments					
Date	Description	Details			Balance
22-Feb-11	A/C Opened				$0.00
25-Feb-11	Opening Deposit	Cheque	$51,070.00		$51,070.00
26-Feb-11	Counter Deposit	Cheque	$58,775.00		$109,845.00
28-Feb-11	Janus Investments Boston	TFR	$56,075.00		$165,920.00
01-Mar-11	Janus Holdings Boston	TFR		$50,000.00	$115,920.00
07-Mar-11	R J Janus	TFR		$51,770.00	$64,150.00

Account Holding Branch: London					
Account Name: R J Janus					
Date	Description	Details			Balance
05-Mar-11	A/C Opened				$0.00

05-Mar-11	Opening Deposit	Cheque	$110,812.50	$110,812.50
07-Mar-11	Janus Investments Dubai		$51,770.00	$162,582.50

Here we have four bank accounts, held at three different branches of Pecunia Bank. The account names ('Janus Investments' in Dubai, 'Janus Holdings' in Boston and 'R J Janus' in London) are different, but are all quite similar. It is possible, therefore, that the ownership of these accounts might be connected. The fact that money has been transferred between these accounts strengthens the perception that there may be a connection in their ownership.

Client ownership of multiple accounts in different branches of the same bank is one of several behaviours that has been identified as potentially suspicious by the Financial Action Task Force. Questions that might need to be asked about such accounts include the following:

- Does there appear to be a legitimate purpose for these multiple accounts, other than the moving around of funds?
- Is there any economic purpose to the transfers of money made between such multiple accounts?

The movements between the various accounts don't appear to make much sense at all. For example, why would 'Janus Investments' in Dubai need to receive $56,075.00 *from* 'Janus Investments' in Boston, only to transfer $50,000.00 back *to* 'Janus Holdings' in the Boston branch of Pecunia Bank the following day? Such transactions do not make sense, seem to serve no economic purpose and should give grounds for suspicion.

Sample Account 8

Account Holder: PRLC Legal & Financial Consultants					
Date	Description	Details	Receipts	Payments	Balance
01-Feb-11	Balance C/F				€118,445.32
08-Feb-11	Invoice 39476	REM	€6,782.45		€125,227.77
10-Feb-11	Invoice 39480	REM	€2,938.05		€128,165.82
15-Feb-11	Invoice 39481	REM	€1,394.54		€129,560.36
15-Feb-11	Kubik Camden & Partners	TFR		€1,293.45	€128,266.91
17-Feb-11	Invoice 39482	REM	€3,456.21		€131,723.12
22-Feb-11	Invoice 39483	REM	€3,342.53		€135,065.65
26-Feb-11	Salary account	TFR		€1,862.89	€133,202.76
26-Feb-11	Tubacon SA, Roma	TFR		€50,435.56	€82,767.20
27-Feb-11	Invoice 39484	Cash	€68,495.45		€151,262.65
01-Mar-11	Invoice 39485	REM	€3,094.54		€154,357.19
01-Mar-11	Nortran (Office Rental)	TFR		€3,405.00	€150,952.19
03-Mar-11	Invoice 39486	Cash	€54,606.35		€205,558.54
05-Mar-11	Invoice 39487	Cash	€74,523.54		€280,082.08
05-Mar-11	Invoice 39489	REM	€3,424.12		€283,506.20
09-Mar-11	Invoice 39488	Cash	€34,958.76		€318,464.96
11-Mar-11	Invoice 39478	REM	€8,795.34		€327,260.30
11-Mar-11	Invoice 39490	REM	€4,958.54		€332,218.84
11-Mar-11	Tubacon SA, Roma	TFR		€85,402.32	€246,816.52
18-Mar-11	Invoice 39479	REM	€4,938.45		€251,754.97
25-Mar-11	Invoice 39477	REM	€15,837.67		€267,592.64
26-Mar-11	Salary account	TFR		€1,862.89	€265,729.75
27-Mar-11	Invoice 39491	REM	€2,493.56		€268,223.31
27-Mar-11	Tubacon SA, Roma	TFR		€97,495.34	€170,727.97
28-Mar-11	Invoice 39492	Cash	€54,495.45		€225,223.42

This appears to be a legitimate consultancy business, but if you look at the pattern of transactions something is not quite right about the invoices that have been issued to and apparently paid by clients:

- Invoices up to and including Invoice 39483 were all paid by electronic transfer.
- The amounts invoiced up to and including Invoice 39483 are all below €16,000.
- Invoice 39484 is for a much larger amount (€68,495.45) and has been paid in cash.
- From this point forward, more than half the invoices issued are for these much larger amounts and, wherever these larger amounts occur, the invoice is invariably settled in cash.

This change in transaction behaviour appears to have no legitimate explanation. Has this business suddenly got itself involved in money laundering? The change in invoiced amounts and the shift towards cash settlements could be indicative of this. The FATF specifically identifies a shift towards cash transactions (where previously these did not happen) as an indicator of potential suspicion.

Sample Account 9

Account Holder: J Gregor					
Current Account					
Date	Description	Details	Receipts	Payments	Balance
01-Jan-05	A/C Opened				$0.00
24-Jan-05	Haverton Retail	REM	$717.10		$717.10
25-Jan-05	Withdrawal	ATM		$325.00	$392.10
01-Feb-05	J Gregor Account 10545463	TFR		$200.00	$192.10
12-Feb-05	Cash Withdrawal	ATM		$150.00	$42.10
24-Feb-05	Haverton Retail	REM	$717.10		$759.20
25-Feb-05	Cash Withdrawal	ATM		$325.00	$434.20
01-Mar-05	J Gregor Account 10545463	TFR		$200.00	$234.20
17-Mar-05	Cash Withdrawal	ATM		$150.00	$84.20
24-Mar-05	Haverton Retail	REM	$717.10		$801.30
25-Mar-05	Cash Withdrawal	ATM		$325.00	$476.30
01-Apr-05	J Gregor Account 10545463	TFR		$200.00	$276.30
15-Apr-05	Cash Withdrawal	ATM		$150.00	$126.30
24-Apr-05	Haverton Retail	REM	$717.10		$843.40
25-Apr-05	Cash Withdrawal	ATM		$325.00	$518.40
16-May-05	Cash Withdrawal	ATM		$150.00	$368.40
24-May-05	Haverton Retail	REM	$717.10		$1,085.50
25-May-05	Cash Withdrawal	ATM		$325.00	$760.50
01-Jun-05	J Gregor Account 10545475	TFR		$275.00	$485.50
15-Jun-05	Cash Withdrawal	ATM		$150.00	$335.50
24-Jun-05	Haverton Retail	REM	$717.10		$1,052.60
25-Jun-05	Cash Withdrawal	ATM		$325.00	$727.60
01-Jul-05	J Gregor Account 10545475	TFR		$275.00	$452.60
17-Jul-05	Cash Withdrawal	ATM		$150.00	$302.60
24-Jul-05	Haverton Retail	REM	$717.10		$1,019.70
..... several months later.....					$0.00
01-Nov-05	J Gregor Account 10594832	TFR		$300.00	$346.00
14-Nov-05	Cash Withdrawal	ATM		$175.00	$171.00

24-Nov-05	Haverton Retail	REM	$717.10		$888.10
25-Nov-05	Cash Withdrawal	ATM		$325.00	$563.10
01-Dec-05	J Gregor Account 10594832	TFR		$300.00	$263.10

Loan Accounts

Date	Description	Details	Receipts	Payments	Balance
01-Jan-05	A/C Opened			$18,000.00	−$18,000.00
31-Jan-05	Interest	DD		$75.00	−$18,075.00
01-Feb-05	J Gregor Account 10545463	TFR	$200.00		−$17,875.00
28-Feb-05	Interest	DD		$75.00	−$17,950.00
01-Mar-05	J Gregor Account 10545463	TFR	$200.00		−$17,750.00
31-Mar-05	Interest	DD		$75.00	−$17,825.00
01-Apr-05	J Gregor Account 10545463	TFR	$200.00		−$17,625.00
02-Apr-05	Loan Repayment	Cash	$17,625.00		$0.00
01-May-05	A/C Opened			$37,500.00	−$37,500.00
31-May-05	Interest	DD		$156.25	−$37,656.25
01-Jun-05	J Gregor Account 10545475	TFR	$275.00		−$37,381.25
30-Jun-05	Interest	DD		$156.25	−$37,537.50
01-Jul-05	J Gregor Account 10545475	TFR	$275.00		−$37,262.50
31-Jul-05	Interest	DD		$156.25	−$37,418.75
01-Aug-05	J Gregor Account 10545475	TFR	$275.00		−$37,143.75
01-Aug-05	Loan Repayment	Cash	$37,143.75		$0.00
01-Sep-05	A/C Opened			$45,000.00	−$45,000.00
30-Sep-05	Interest	DD		$187.50	−$45,187.50
01-Oct-05	J Gregor Account 10594832	TFR	$300.00		−$44,887.50
31-Oct-05	Interest	DD		$187.50	−$45,075.00
01-Nov-05	J Gregor Account 10594832	TFR	$300.00		−$44,775.00
30-Nov-05	Interest	DD		$187.50	−$44,962.50
01-Dec-05	J Gregor Account 10594832	TFR	$300.00		−$44,662.50
03-Dec-05	Loan Repayment	Cash	$44,662.50		$0.00

This example demonstrates the use of loan accounts as a vehicle for

laundering money:

- The customer takes out a loan.
- They pay a few instalments on the loan as arranged.
- They suddenly produce the cash funds to clear the loan.
- The loan account is closed.

Unless there is a reasonable explanation for the source of the funds used to pay off the loan, this has to be regarded as suspicious.
In this example, the customer has in fact taken out three separate loans, one after the other. In each case, the loan payments are made as normal for the first three months. At the end of three months, the customer suddenly makes a cash repayment for the outstanding balance of the loan. For the first loan, the cash balance paid was, $17,625.00. For the second loan, the amount paid in cash was $37,143.75. For the third loan, the cash repayment was $44,662.50. The customer receives a regular payment of $717.10 from Haverton Retail and has no other apparent sources of income, which is nowhere near enough money to pay off any of these amounts in one go.
Note: a training film dealing with money laundering through loan accounts can be previewed at http://www.antimoneylaunderingvideos.com/player/red_flags_aml.htm.

Sample Account 10

Account Holder: Curanic Commercial Services (London)					
Current Account					
Date	Description	Details	Receipts	Payments	Balance
01-Jan-04	A/C Opened				€0.00
24-Jan-04	Hipocanthus Financing Prague	REM	€112,500.00		€112,500.00
25-Jan-04	Counter Withdrawal	Cash		€14,500.00	€98,000.00
01-Feb-04	Aramis Consulting	TFR		€23,000.00	€75,000.00
12-Feb-04	Counter Withdrawal	Cash		€13,900.00	€61,100.00
26-Feb-04	Anapolis Professional Services	REM		€25,043.00	€36,057.00
03-Mar-04	Cash Withdrawal	ATM		€14,755.00	€21,302.00

Curanic Commercial Services has taken receipt of a large amount of money from a third party account overseas. There are no further deposits to the

account, but a substantial number of withdrawals. Some of these withdrawals are in the form of transfers to third-party businesses with vague and non-specific names, such as ‘Aramis Consulting’ and ‘Anapolis Professional Services’. In short, Curanic does not appear to do a lot other than transfer money around. It receives money from overseas, and it moves money on to other third parties. This behaviour is typical of a shell company, which has no business purpose other than to act as a conduit for the receipt and transfer of funds.
The receipt of large sums from abroad, followed by large numbers of withdrawals is one of the patterns of behaviour identified by the Financial Action Task Force as an indicator of potential suspicion.

‘ACCUMULATION OF EVIDENCE’ CASES

Suspicion can be something that grows. The exact time at which one moves from an attitude of caution or uncertainty into one of suspicion is a moot point. The following cases address that issue.
Each case study has five stages, so that the relevant information builds to form a complete picture. Read each stage and consider your reactions to it. Is there anything unusual, unexplained or which goes against what you might expect to see in an account of that nature? Do this for each stage, then check your reactions against the comments that appear at the end of each case.

Case 1: Feron Resources

Stage 1

Feron Resources first opened an account with your bank when it was incorporated as a company five years ago. The company provides business administration and accounting services and consultancy. It currently employs 20 people, and has a client base of approximately 50 companies, most of which are small, privately owned businesses.

Stage 2

About six months ago, Feron Resources underwent a change of ownership. The previous owners were well known to your bank. The new owner is a corporation called ‘Commercial Enterprises’. The owner of this corporation is given as a consortium of wealthy entrepreneurs, all well-known public figures but with no previous history or relationship with your bank.

Stage 3

In the past five months Feron has acquired several new and extremely profitable clients. These companies all buy an extensive range of services from Feron. The amounts invoiced to them has increased month by month, until in the last month they accounted for roughly 50 per cent of Feron’s total income. None had done business with Feron previously.

Stage 4

Although the invoiced volume of business has increased substantially in the past six months, there has been no real change in staffing levels, and staff themselves do not seem aware of a change in the volume of work. The only new recruit to the company has been Ms Yeretzi who was appointed by the new owners to manage their business on their behalf.

Stage 5

Feron’s recent outgoings include several substantial payments to a company called Infotek. These payments are recorded in Feron’s accounts as ‘consultancy fees’, ‘business development fees’, or simply ‘fees’. When the bank enquired, the only person who had any knowledge of Infotek was Ms Yeretz, and she was unavailable.

Observations

Feron Resources

Stage 1

There is nothing particularly suspicious or alarming here. In fact, it seems clear that Feron has been operating as a perfectly legitimate

business for a number of years. The business seems quite healthy, there is nothing to suggest any wrongdoing.

Stage 2

The change of ownership is a possible cause for concern, although the owners in question are well-known public figures and the bank presumably knows quite a lot about their reported activities. However, the bank has no previous banking experience of these individuals, and no direct knowledge of these people's banking habits, or of their actual assets. What is the association between them? What is 'Commercial Enterprises', and what does it do? Why is 'Commercial Enterprises' interested enough in Feron Resources to want to own it? These are all important questions.

Stage 3

There is evidence here of a change in Feron's business pattern, and this change coincides with the new ownership. Where do these new clients come from? Why are they suddenly interested in doing business with Feron? Why do they seem to buy substantially more from Feron than any other client (they have 50 per cent of the business, and yet they constitute only a small proportion of the total client base)? Does this change in the pattern of business seem legitimate?

Stage 4

Even though the volumes invoiced would suggest a greatly increased volume of business, this does not appear to be reflected in Feron's staffing patterns. Could it be that Feron is using false invoices as a cover

for receiving criminal money? Does Feron *really* do the work for which these companies have been invoiced?

Stage 5

The relationship with Infotek is not clear. What is Feron *really* buying from Infotek? What service is it getting in exchange for the fees apparently paid to Infotek? Or is Feron simply being used as a vehicle through which to channel criminal money back to its criminal owners, hiding behind the name of Infotek? Also, who is the mysterious Ms Yeretz? Is she an innocent employee, or is she knowingly supervising a money laundering operation?

Case 2: Mr Julian Chellis

Stage 1

Mr Chellis is a resident citizen and wishes to open a personal account, with an opening deposit of €5,000. He would like the account to be set up immediately, so he can take receipt of a payment he is expecting. He is unable to visit the bank right now as he is overseas but he will visit the bank to complete the documentation later.

Stage 2

Mr Chellis has now opened his account and completed the documentary requirements, sending his brother initially in order to provide the necessary documents which included a copy of his passport and a mortgage document bearing Mr Chellis' name. The payment that he was expecting (€9,000 from an account overseas) has arrived, but the purpose of the payment and his connection with its originator are not clear. Mr Chellis has been asked to visit the bank to discuss this matter. He seems reluctant to give any additional information about the payment in question, or about his business connections in the overseas country.

Stage 3

It is two months later, and apart from the opening deposit of €5,000 and the €9,000 received from the overseas country, there has been very little activity on Mr Chellis' account. In the past three weeks, however, the account has received deposits of more than €53,000 from three other third-party accounts outside the country.

Stage 4

Mr Chellis' account has received a further €15,000 in various instalments this time from an account in his name from outside the country. You have checked Mr Chellis' account application and you see that he has no declared overseas business interests. His account also shows no regular payments from overseas relatives. Yet he has received a total income from overseas of tens of thousands in the past two to three months

Stage 5

Over the past ten days, Mr Chellis has ordered five wire transfers to different overseas accounts in third-party names. Each wired amount is €9,800. Mr Chellis has just contacted the bank to inform it that he wishes to close his account, and for the bank to prepare a banker's draft for the outstanding deposit in the account, to be collected on his behalf by his brother.

Observations

Mr Julian Chellis

Stage 1

Mr Chellis is putting pressure on the bank to provide him with banking services *before* he has properly identified himself or provided any proof of identity.

Stage 2

Is Mr Chellis really unable to attend the bank, or is it simply that he does not want to be identified? Any apparent reluctance to meet banking staff might be considered suspicious. Also, the use of an intermediary is one of several ploys which might be used by a person to try to keep their true identity hidden (although it is also consistent with a wealthy individual who cannot be bothered with such details). In this case the intermediary has a copy of Mr Chellis's passport rather than the original passport. The copy has not been certified and may not, therefore, be authentic. Copies are easily forged and banks usually protect against this, by requiring to see either the original document itself or at the very least a certified copy. Finally, the mortgage agreement presented as proof of Mr Chellis's residence is useful in proving that he has a house, but does *not* prove that he actually lives in it. He could be living anywhere. Information about a customer's permanent residence is one of the key pieces of identifying information that needs to be obtained by banks, when opening new accounts.

Stage 3

Mr Chellis's account has lain dormant for some time, but has suddenly become very active. The account has received substantial deposits, and it is unclear whether these deposits are consistent with Mr Chellis's legitimate employment or business. Does he really earn or have legitimate access to this amount of money and why is it coming to him? The deposits received by Mr Chellis come from three accounts outside the country but there is no indication as to what Mr Chellis's relationship is with the third parties who remitted the funds.

Stage 4

This information confirms that Mr Chellis is now receiving deposits from overseas accounts in his own name, despite there having been no indication of this when he opened his account. This is therefore unexplained activity, it needs to be investigated and, if credible explanations cannot be established, treated as suspicious.

Stage 5

Mr Chellis has suddenly decided to empty and close the account. Rather than have the money transferred to an account in his name elsewhere, he has asked the bank to produce a banker's draft for the amount. Banker's drafts are drawn on the bank's deposits rather than on a specific customer account, so when this money is next paid into an account it will be difficult to identify Mr Chellis as the source. Also, Mr Chellis still seems very reluctant to come into the bank – he has sent his intermediary along to collect the banker's draft.

THE 21ST CENTURY: AREAS OF RISING CONCERN

As the world changes around us the opportunities for criminal enterprise are constantly changing too.

- The 21st century has seen the re-emergence of slavery in its modern-day form, through human trafficking and the exploitation of its victims.
- The rise of the cryptocurrency has opened the door to new ways to launder money and commit financial crime.

- The use of the globalised economy and networked financial system by corrupt government officials to launder the proceeds of fraud, corruption and state theft on a grand scale.

In the early 21st century these three topics are very much of our times. Organisations such as FATF and other international institutions have invested hugely in developing our understanding of money laundering in relation to these three areas. The summaries below are intended as an overview of the three topics, their relevance to our time, their interest from a money laundering perspective and some of the red flags to look out for.

Human smuggling, human trafficking, modern slavery and money laundering

Wherever human smuggling and trafficking crimes are being committed, money laundering is never far away. In a 2011 report FATF confirmed that, '... there is growing evidence that criminals are turning to trafficking in human beings (THB) and the smuggling of migrants (SOM) to a greater extent as these crimes are seen as highly profitable'. And the problem is becoming more prevalent. A July 2018 report by FATF ('Financial Flows from Human Trafficking') states that '... an estimated 24.9 million people were in forced labour and sexual exploitation at any moment in time in 2016', with the numbers continuing to increase yearly. The International Labour Organization (ILO) has estimated the total illicit proceeds from human trafficking to stand at USD 150.2 billion in 2018.
Human smuggling and human trafficking are connected, but nonetheless different. The US Financial Crimes Enforcement Agency (FINCEN) explains the difference as follows:
Human smuggling:

- involves persons choosing to immigrate illegally
- is limited to illegal migration or the harbouring of undocumented aliens
- involves foreign nationals
- involves an illegal border crossing or the harbouring of someone that has illegally entered a country.

Human trafficking:

- involves the use or force or coercion and the exploitation of victims
- involves, but is not limited to, involuntary servitude, forced labour, debt bondage, peonage and sexual exploitation
- anyone can be a victim regardless of origin, sex, age or legal status
- there is no need for a person to cross a border to be trafficked; individuals can be trafficked within the borders of a country.

The connection between the two is that individuals who 'choose' to be smuggled often ultimately end up as coerced victims of trafficking. In recent times the persistence and ferocity of political conflict across, in particular, the African and Arabic world has fed a spiralling refugee crisis which, in turn, has given rise to increases in human trafficking, slavery and exploitation. With hundreds of thousands – millions, going forward – of vulnerable people seeking to flee conflict and corruption for safer havens and better opportunities elsewhere, the opportunities for unscrupulous criminal gangs to exploit the situation are vast.

The human beings who are being smuggled and then exploited are desperate and prepared to risk all for the chance of a better life. Many borrow large sums of money to pay the smugglers, with little or no prospect of ever being able to repay what they have borrowed. They become 'chattels' of the gangs, forced to live and work in appalling conditions as sex workers or simply as 'slaves', in lieu of repaying their debt.

The traffickers obviously need to move funds across borders to fund their operations. They also need mechanisms to retrieve and launder the profits of their trafficking activities. As with other serious crime it is important to understand the kinds of financial transactions involved, so we are better able to recognise them and take appropriate action.

One of the difficulties in identifying transactions that have a human smuggling or human trafficking connection is that we are dealing with a chain of criminal activities, each having its own financial characteristics.

Payment to smugglers

Smugglers may take full payment in advance, partial payment prior to departure with the remainder paid on arrival, or they may enter into an arrangement where the relatives of the migrant pay up in full in the origin country once the migrant has arrived safely at their destination.

Example

Ahmed has fled Syria and used the services of a people smuggling ring to find his way to Germany, where he has been granted asylum and residency as a refugee. Ahmed has a job in his new country of residence and makes regular payments back to his home country of Syria. The payments are not to known members of his family or anyone else with whom he has a known, legitimate association. The payments are to an apparently unconnected third party – in fact the 'money man' of the people smugglers whose job it is to collect payment.

Recruitment or abduction

Where trafficking is concerned, the victims are often entrapped through deception or force. People smuggling is a common route in for the traffickers as individuals who cannot pay the smugglers are forced to work to pay off the debt. But traffickers are also known to use other methods of deception, for example extortion by threatening to harm the relatives of smuggled individuals back home, or the use of false marriages, kidnapping or advertisements purporting to offer employment or study opportunities abroad.

These activities may also leave their financial trace for those who know what to look for.

Transportation of human 'assets'

The smugglers and traffickers need to move their human subjects around and will incur financial costs in the process.

Example

Mr Raler's bank account details identify his occupation as 'retired company director'. His account shows frequent multiple payments for airline tickets

and hotels for different named women. Mr Raler is the agent of a trafficking gang with responsibility for bringing each new group of victims under false pretences from their country of origin to the UK, where they will be exploited. One of the women for whom he recently purchased air travel is called Andrina. She is travelling to the UK to work and has no previous known association with Mr Raler.

Exploitation of victims

The exploitation of victims can create a distinct financial pattern which, if it does not fit with usual or expected activity, should give rise to suspicion.

Example

Andrina has travelled from Russia to the UK on the promise that legal employment will be waiting for her. Mr Raler, the agent who arranged her employment, said that his 'agency' would cover her travel and her accommodation and living costs once in the UK. On arriving in the UK, she has discovered that there is no job and that the costs incurred on her behalf are now a 'debt' that she has to repay. The punitive interest on this debt in effect means that she will never be able to repay it. She is forced to work as a sex worker. The traffickers have threatened both her and her family back home if she refuses to work or tries to escape. They are confident in her compliance and, as part of the tools for her sex work, they have provided her with a mobile phone and a bank card. Andrina receives instructions via her mobile on where to go to meet with each client that has been assigned to her. She uses the bank card to cover her expenses – taxi fares to get from one appointment to the next, food and supplies such as condoms. The pattern of transactions made using her bank card is as follows:

- she has incurred a large number of late-night taxi fares
- she is moving around the country a lot, staying in each city for just a few days at a time
- although not resident in the places she stays, she does not appear to incur accommodation costs
- she does, however, incur room service bills at various motels and hotels where she is not a registered guest
- she is also visiting fast food establishments and pharmacies several times a day.

In association with the unusual card transactions Andrina's account also receives frequent email money transfers from multiple different email addresses all with male names. She also makes frequent fund transfers to a third-party account in the name of Mr Smith, or a company controlled by him.

Detection of these patterns may well be beyond the capabilities of individual bank employees and traditional rules-based transaction surveillance systems. But the good news is that identifying and highlighting these patterns is exactly the kind of thing that the AI-enable systems starting to come onstream now excel at, thus giving us powerful new capabilities for detection and reporting going forward.

Laundering of illicit proceeds of trafficking

At the top of the structure, of course, are the organisers of the trafficking – the ultimate beneficiaries of Andrina's and her co-workers' enforced labour.

Example

Mr Smith's account is largely funded by email money transfers from Andrina and a host of similar individuals. The funds received are not consistent with his known income and sources of wealth. Received funds are quickly moved on via cash transfers, credit card payments and third-party payments to other individuals and entities.

The types of transactions you would see at this level are no different from money laundering in relation to any other crime. This is the receipt and distribution account. The proceeds of crime passing through this account are quickly transferred on to other third parties and dispersed for further laundering.

Possible red flags

FATF in fact assert that no specific guidance has been issued on red flag indicators for money laundering associated with human smuggling and trafficking because '... the channels used, the instruments and sectors implied are the same as for other criminal activities'. This is not surprising when you think about it – those involved in human smuggling and trafficking are often intermingled with other serious crimes such as drug-trafficking and protection racketeering, so it is logical that many of the same money laundering methods would be used as for other crimes. Even so, FATF, FINCEN and others have identified certain financial transaction patterns that are specific red flags for the victims of people smuggling and human trafficking. These include the following:

- use of Money Service Businesses (MSBs) by migrant workers transferring a part of their salaries to apparently unconnected third parties abroad, in payment of a debt
- frequent payments to online escort services for advertising including online classifieds as well as more expensive, higher-end

advertising and website hosting

- frequent transactions carried out by a business customer in apparent efforts to provide sustenance to individuals (e.g. payment for housing, lodging, regular vehicle rentals, purchases of large amounts of food), where such transactions are inconsistent with the known nature of the business
- payments to employment or student recruitment agencies that are not licensed or legally registered
- women who transfer small sums to relatives while passing the larger portion to other third parties (i.e., the people behind the trafficking)
- customers depositing funds under an escort (as revealed by CCTV footage)
- customers who provide a telephone number that can be linked to personal services ads through open sources such as Google
- new customers arriving from high-risk countries and making frequent major transactions
- people and entities that can be linked to prostitution and whose transactions exceed their known income or wealth in value
- rental and other payments against addresses known to be associated with sex work
- multiple payments for different women for airline tickets and hotels
- letters of employment provided by employment agencies acting for known high-risk sectors such as agricultural work, food processing and manufacturing
- use of a single mobile number and address to open multiple accounts in different names

- use of multiple bank accounts and credit cards.

Cryptocurrencies

Cryptocurrencies have been on the rise since the late 2000s and the number of businesses dealing in them, offering services related to them and/or raising funds for projects involving them, is growing rapidly. There are a number of features of note.

- As noted in Chapter 2, in many jurisdictions' cryptocurrencies are subject to minimal regulatory oversight (although this is starting to change, with some jurisdictions now starting to develop frameworks for the regulation of cryptocurrency markets).
- Cryptocurrency accounts may not be insured and deposits may therefore not be protected against the failure of the coin itself or the market in which it is traded.
- Cryptocurrencies are hugely volatile and therefore pose major risks, particularly for non-sophisticated investors.
- With minimal regulation in place the companies that trade in cryptocurrencies may be unregulated, lacking in internal controls and therefore more exposed to risk of theft and fraud.

While there are plenty of legitimate uses for and investors in cryptocurrency there are also a number of high-profile cases involving the use of cryptocurrencies in facilitating money laundering.

Example

The Silk Road and Liberty Reserve cases highlighted in Chapter 1 provide classic examples of how the TOR anonymity network, the trade in bitcoin and the use of bitcoin 'tumblers' enabled a market in illegal substances and goods to develop.

In another high-profile case, Western Express International, a New York-based virtual money-changer and unregistered money transmitter played a key role in laundering the proceeds of identity theft cyber-fraud schemes.

There are also a number of instances where cryptocurrencies have been the preferred method of payment in the execution of high-profile frauds or thefts. Ransomware attacks, for example, are threats to online security which set out to extort payments in cryptocurrency from their victims.

Example

One of the largest ransomware attacks was the May 2017 ‘Wannacry’ attack. Wannacry was a piece of malware which affected more than 200,000 systems across more than 150 countries, with the hackers instructing victims to pay a ransom to one of three bitcoin addresses in order to restore access to their files.

Ransomware attacks have in fact increased by 3,500 per cent from 2015 to 2016 and in the same perio dthe ransoms paid increased tenfold (Information-age.com). In March 2019 it was reported that Coinhive was still the most active online threat and cryptomining variants still accounted for half of the top ten most wanted types of malware.
From a criminal perspective of investment fraud, an additional attraction of cryptocurrencies is that they are difficult to understand and beyond the comprehension of average investors, who may not really know about the investment they are buying, how it should perform or even whether or not it is genuine.

Example

In 2019 three fraudsters were indicted by the United States for setting up and operating a multi-billion-dollar Ponzi scheme around a fake cryptocurrency called OneCoin. The company ran as a pyramid marketing operation which offered members a commission for selling OneCoin investment packages. In the period from 2014 investors were defrauded of more than USD 3.8 billion. The company claimed to have its own private blockchain whereas in fact it did not and offered investors no means of tracing their investment. The main figures behind the company also had past history from their involvement in previous similar Ponzi schemes. When asked at a meeting how investors could monetise their investment OneCoin's response was obtuse, aggressive and otherwise unresponsive. The question might also have been raised about how a relatively small group of people were apparently able to operate a company with over USD 3bn in assets.

So what steps can institutional investors take to protect against such scams? And what questions should financial institutions considering onboarding such businesses as clients be asking as part of their enhanced due diligence procedures? Consider the following.

- Are the company's principals of good standing? What is their track record?
- Does the company have a true physical presence, i.e., real company offices at a real company address?
- Does the company's structure make sense, i.e., staff numbers and credentials that truly reflect the size and nature of the business?
- Does the company have expertise relevant to the operation of a cryptocurrency? Can they provide technical documentation or other evidence of how the coin works? Do they have a chief technical officer with the relevant technical background and standing?
- How does the company regulate its cryptocurrency? What transaction records does it keep? How does it track and monitor

movements of the currency?

- What information about their investments can investors pull down, from where and how often?
- Is the company able to explain and substantiate its claims for the potential returns from the investment, and the period over which those returns might be realised?
- Does the company have adequate systems and controls in place commensurate with the nature of the investment and the amount of risk involved?

Possible red flags

Common red flags to look out for include the following:

- inability or unwillingness to provide technical evidence of how the cryptocurrency operates
- inability or unwillingness to provide evidence of the technical history and background of the company's principals
- inability or unwillingness to provide evidence of procedures and controls to regulate cryptocurrency transactions and mitigate risk
- unwillingness to engage with, communicate with or make information available to investors once they have invested
- guarantees offered of unrealistically high returns on investment in cryptocurrencies
- overly aggressive promotion of cryptocurrency investment opportunities, especially offers made via non-physical platforms such as social media
- pressure to buy immediately, act fast or 'get in on the ground floor' with a new technology trend

- investment offers made by unlicensed sellers and/or unregulated firms.

https://www.techspot.com/amp/news/79132-cryptocurrency-malware-most-prevalent-threat-internet-but-slowly.html

http://www.fatf-gafi.org/media/fatf/documents/reports/Trafficking%20in%20Human%20Beings%20and%20Smuggling%20of%20Migrants.pdf

https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2014-a008

http://www.fatf-gafi.org/media/fatf/content/images/Human-Trafficking-2018.pdf

https://www.techspot.com/amp/news/79133-onecoin-cryptocurrency-executive-arrested-multibillion-dollar-fraud.html

https://www.crowdfundinsider.com/2018/01/126665-nasaa-publishes-list-cryptocurrency-concerns-red-flags-fraud/

Financing of terrorist recruitment

In recent years there has been an increasing focus on understanding the methods used by terrorist organisations to recruit and attract new operatives, members and supporters to their organisations. Terrorist organisations are dependent on their recruitment operations for resources and support. The theory goes that, if governments and the international community understand how terrorist recruiting is financed, then they will be better able to impede the recruitment process and reduce the terrorist threat.
A FATF report in January 2018 (‘Financing of Recruitment for Terrorist Purposes’) identifies five main areas of terrorism recruitment expenditure.

These are:

- the payment of personal expenses incurred by the recruiters and/or the recruitment network
- the costs incurred in establishing and equipping a terrorist unit – transportation and accommodation costs and the creation of fake identities
- direct payments made to recruits, mercenaries and civilian experts
- production of recruitment material, both online content and hard print items such as books, magazines and leaflets
- the costs incurred in securing premises to be used for meetings, propaganda events, recruitment fairs and the like.

The report identifies groups who are especially vulnerable and specifically targeted by terrorist recruiters including:

- the very poor, for whom terrorist recruiters are willing to provide basic amenities such as food, accommodation and financial support for their relatives
- inmates in prisons (there is clear evidence of an increase in recruitment and the dissemination of terrorist ideologies within prison communities).

It also identifies the important role played by social media and their emergence over the five years to 2018 as the tools most commonly used by terrorist organisations for recruitment and propaganda purposes. To be able to exploit social media as capably as they do clearly requires a level of expertise and equipment that, presumably, comes at a cost. The difficulties in preventing the dissemination of terrorist propaganda and content via social media was highlighted by the terrorist attacks in New Zealand in March 2019 when a terrorist used a head-mounted GoPro camera to film himself shooting worshippers at two mosques in Christchurch and streamed the content live across social media. Within hours the content had been uploaded and shared hundreds of thousands of times – faster than the social media platforms were able to identify and take the content down.
Terrorist organisations and individuals have not been slow to exploit emerging social media technologies, nor have they been slow to embrace new forms of technology-based financial tools such as e-wallets as a means

of providing financial incentives to recruits or a means of access to funds for operatives in the field.
Crowdfunding is another legitimate, internet-based fund-raising tool that terrorist organisations have been known to exploit for terrorist financing purposes, including financing the travel of foreign terrorist fighters.
Targeting the financing of terrorist recruitment provides the authorities with the opportunity to identify and disrupt terrorist activities at root.
From a suspicion recognition perspective, the key to identifying potential red flags rests with the quality and robustness of institutions' 'know your customer' procedures. Terrorist-linked financial transactions may not be unusually large, complex or notable. Many of them will look much the same as the transactions of ordinary people, going about the ordinary day-to-day business of working and living. How, then, can institutions distinguish between these normal everyday transactions and the sinister, more darkly intended transactions of terrorist-connected individuals? The answer rests in what you know about the individual in question – what looks normal and abnormal for them, given what you know about their background, circumstances and sources of income.

Grand corruption, fraud and theft of state assets

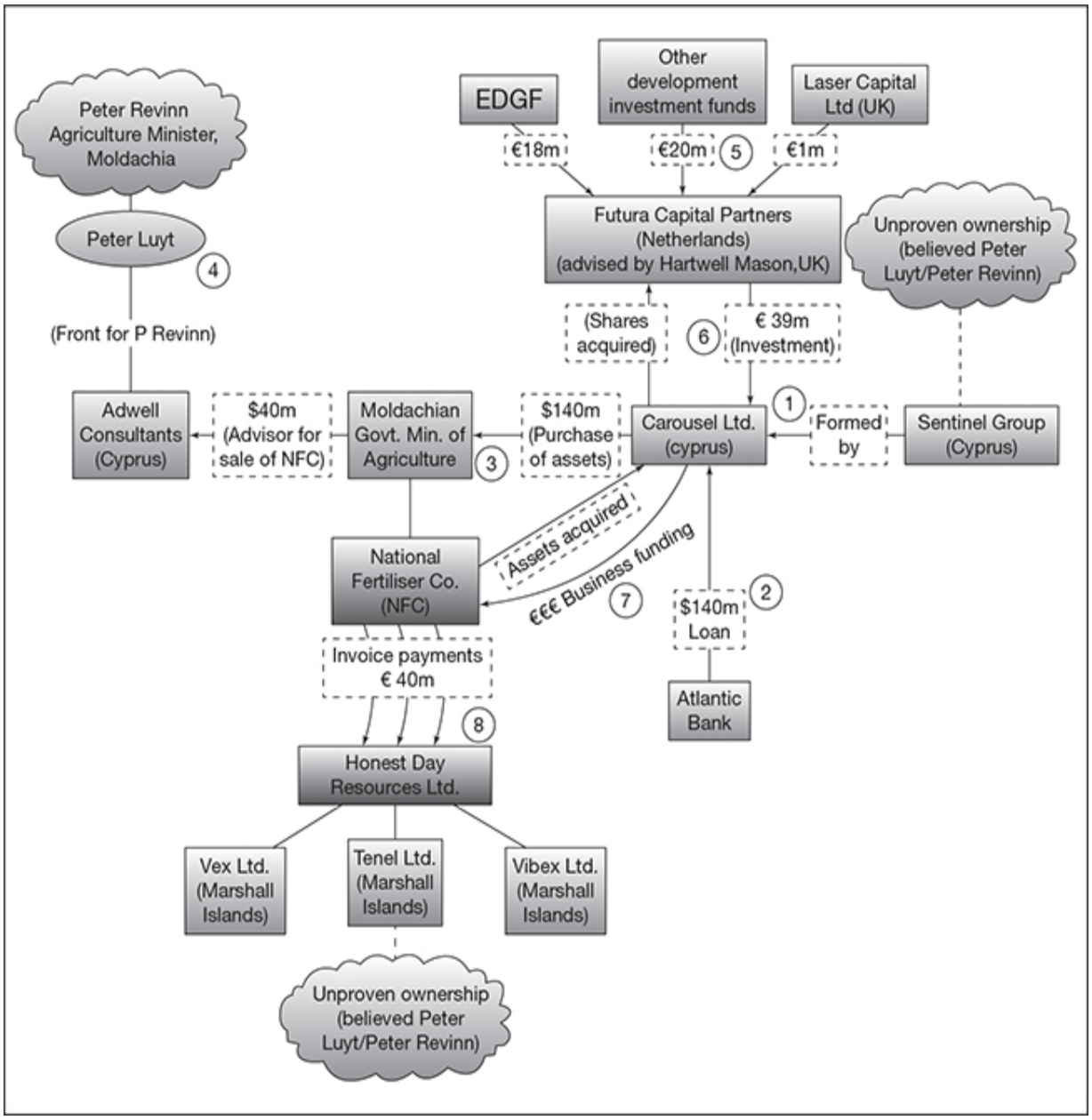
The World Bank estimates that upwards of USD 1.5 trillion equivalent is paid in bribes to corrupt government officials for the award of business contracts. According to the World Bank, again, the prevalence of corruption, particularly in developing economies is associated with:

- suppressed, static or reducing incomes (successful attacks on corruption increase incomes by 400 per cent)
- increased child mortality (dealing successfully with corruption reduces child mortality by 75 per cent)
- slower growth in the business sector (reducing corruption levels can increase business growth by 3 per cent year on year)
- reduced foreign investment (corruption equates to a 20 per cent tax to foreign investors)
- poorer people pay a higher pro-rata percentage of their income to 'The Corruption Tax'.

It was seen earlier on in Chapter 1 with the Russian Laundromat and - Hermitage Asset Management cases, how shell companies with hidden beneficial ownership, nominee directors and shareholders, and with access to multiple bank accounts operated by screens of law firms, accountants and tax consultants, can be used to move and hide assets derived.

Below is a case study comprising a number of commonly occurring elements and which shows how, in countries where corrupt politicians are able to roam unchecked, and who are courted and marketed to by banks, development institutions and professional advisers keen to do deals, both fraud and grand corruption, together in the same scheme, can be taken to great heights. It looks a little complex to start with, but actually it's breathtakingly simple.

Figure 6.2 Carousel Ltd: Fraud, Corruption and Money Laundering



Source: © Lessons Learned Ltd 2019

Case study

In Figure 6.2 the UBO of the scheme is a corrupt Agriculture minister in the imaginary country of Moldachia, Peter Revinn, who uses a South African national, Peter Luyt, as a 'front' and consultant. Following the numbering in the diagram, the scheme works as follows.

1. Using nominee shareholders and directors, Revinn and Luyt form and register Sentinel Group in Cyprus, which in turn forms and owns another Cypriot company, Carousel Ltd, whose purpose is to bid in the forthcoming privatisation of the Moldachian National Fertiliser Company (NFC) – currently owned by the Moldachian government and managed by Revinn's Ministry of Agriculture.
2. Carousel obtains a USD 140m loan from Atlantic Bank for the purpose of bidding in the privatisation.
3. In a rigged bidding process, Carousel is successful in its bid, and duly pays $140m to the Moldachian Government in return for the assets and business of the NFC. Revinn has effectively sold the company to himself. Key regulators and/or law enforcement officials with responsibility for oversight in Moldachia are paid off with bribes.
4. As part of the privatisation process, the Ministry of Agriculture hires a consulting firm, Adwell Consultants Ltd, again registered in Cyprus, to advise on the sale, which charges fees of USD 40m. Adwell's (hidden) UBOs are Peter Revinn and Peter Luyt. The advisory fee of $40m represents a straight theft of $40m from the Moldachian taxpayer. (NB The use of consulting and intermediary firms in this way as conduits for the enrichment of public officials is commonplace. Firms bidding for contracts pay bribes disguised as consulting fees to intermediaries and advisers who then feed the payments back to corrupt officials in return for a percentage 'cut' of the payment. Bribe-payers therefore don't need secret accounts for 'slush funds', as the bribes are built into the transaction structure. If well disguised, they may even be tax-deductible against profits for advisory services received.)
5. The scheme continues. Via a Dutch fund manager, Futura Capital Partners (FCP), advised by an English law firm, Hartwell Mason, Carousel obtains equity investment funds of $39m from a mixed group of investors – the European Development Fund Group (EDFG), Laser Capital Ltd and some other development investment groups.
6. These investment monies are transferred over to the business bank accounts of NFC (now effectively owned and controlled by Revinn and Luyt, through Carousel) for the purpose of 'modernising and growing the business of NFC, to bring it into the 21st century'.
7. Of course, nothing of the sort takes place. The investment monies are stripped out of NFC through a series of invoices for fake services and

non-existent or grossly overvalued goods submitted to the company by Honest Day Resources Ltd, whose registered owners are Vex Ltd, Tenel Ltd and Vibex Ltd, all incorporated in the Marshall Islands, and whose (again, undisclosed) UBOs are – you've guessed it – Peter Revinn and Peter Luyt. Pretty soon, NFC becomes insolvent, its workers are made redundant, Moldachia no longer has a functioning fertiliser industry, Atlantic Bank's loan has to be written off and the equity investors have lost everything. All of the proceeds of the frauds will have been laundered through the accounts, variously, of Carousel, Adwell, NFC, Honest Day, Vex, Tenel and Vibex.

There is a proliferation of such companies in the world, and the warning signs of money laundering activity are clear:

- small companies, newly incorporated
- unclear business purposes and activities
- nominee shareholders and directors
- very large funds flows, received and remitted, for the known size of the company
- funds received from government accounts in countries known for high levels of corruption.

An actual case, that of a Nigerian citizen James Ibori which bore many of the hallmarks of the above, was described in a FATF report at http://www.fatf-gafi.org/media/fatf/documents/reports/Specific%20Risk%20Factors%20in%20the%20Laundering%20of%20Proceeds%20of%20Corruption.pdf

7

International Cooperation

Background

Modern structures of organised crime and terrorism

Mechanisms and tools of international cooperation

International cooperative bodies

BACKGROUND

International cooperation is the mainstay of international efforts and is referred to time and time again in many of the international conventions and treaties mentioned in Chapter 2, which contain many provisions designed to mandate or encourage it. The phrase refers to the capability and willingness of different parts of the world to assist each other in the task of bringing criminals and terrorists to justice, depriving them of the fruits of their crimes and preventing their attacks upon society. This has become even more important with the expansion of so-called 'TransNational Organised

Crime' (TNOC) and international terrorism. International cooperation can occur at the state/governmental, agency or institutional/individual level.

Example

State/Governmental level

The governments of two countries agree a bilateral treaty of extradition, meaning that a person who is alleged to have committed a crime in Country A, but who is currently physically present in Country B, can be legally transported or 'extradited' from Country B to Country A in order to stand trial.

Agency

Information on the same trading company is shared between Financial Intelligence Units (FIUs) and police forces from three countries regarding Suspicious Activity Reports (SARs) which all three FIUs have received independently from financial institutions in their countries, regarding large 'in and out' deposits. This information is in turn shared with authorities in a fourth country, where the trading company is incorporated and has staff, leading to a coordinated asset seizure across all countries and the prosecution of two of the company's directors for money laundering.

Institutional/Individual

A Compliance Officer within X Bank receives an internal SAR regarding the deposit of an unusually large sum by B Bank, a small bank based in an offshore jurisdiction, which only recently underwent and passed client acceptance checks. Simultaneously, X Bank receives notification from a third party that the money represents the proceeds of a fraud, and that the deposit is an attempt to launder the proceeds, using X Bank as a conduit for

the stolen funds. Together with X Bank's in-house lawyer, X Bank's Compliance Officer speaks to the Compliance Officer of the third party's bank, Y Bank, and obtains important information which enables it to freeze the funds received, and make a full report to the FIU.

The Financial Action Task Force (FATF) has published a number of such examples of international cooperation, demonstrating that when governments, agencies and financial institutions cooperate across borders in the spirit intended by the various treaties and conventions, then it is possible for successes to be achieved, despite the formidable obstacles posed by the existence of multiple jurisdictions.

However, at the state, agency and institutional levels, experience points to a number of serious barriers to achieving the level of international cooperation which is actually necessary to facilitate the effective combating of transnational organised crime. On the face of it, in theory it should be in all parties' interests to cooperate to the maximum degree possible, yet conversations with law enforcement officials reveal continuing challenges in achieving international cooperation.

The barriers identified include:

- *Corruption* – do you trust the other country's police with the information you are giving them? Can offenders bribe judges to refuse requests for assistance and will this compromise your own investigation?
- *State complicity* – where nations may actually benefit economically from the crimes complained of (e.g. the economic benefit derived by the military junta in Burma from the production of opium, or the way in which the Taliban derived revenue from Al-Qaeda when it was hosting Al-Qaeda in Afghanistan).
- *Politics* – governments can oppose mutual assistance on political grounds (e.g. dislike of another country's foreign policy or when trying to extract concessions during international negotiations).
- *Sovereignty* – closely connected to politics, this is where national pride and historical enmities come into play; effectively, disliking another country and what it stands for, more than you dislike your own criminals.

- *'Turf'* considerations at the agency level – sometimes members of an agency in one country dislike the idea that agencies from another country should be getting involved in their affairs. It is a case of 'this is my area, you can't tell what me to do'.
- *Conflicts of laws* – this is a major problem and very complex to resolve. Conflicts of laws occur where what is legally defined as a crime in one country is not a crime in another, or where a defence applies which would not be available in the other country, or where observing the law in one country would entail breaching it in another (e.g. bank secrecy laws) or where enforcement in one country is viewed as being harsh/immoral/illegal in another country (e.g. the death penalty).
- *Breach of contract and poor customer relations* – at the institutional level, many financial institutions are reluctant to extend cooperation across borders to other financial institutions for fear that their actions may result in legal action by their own customers against them. For example, this may occur when a bank is requested to release information regarding a customer's account by another institution (breach of confidentiality) or when it is requested to freeze an account (breach of mandate).

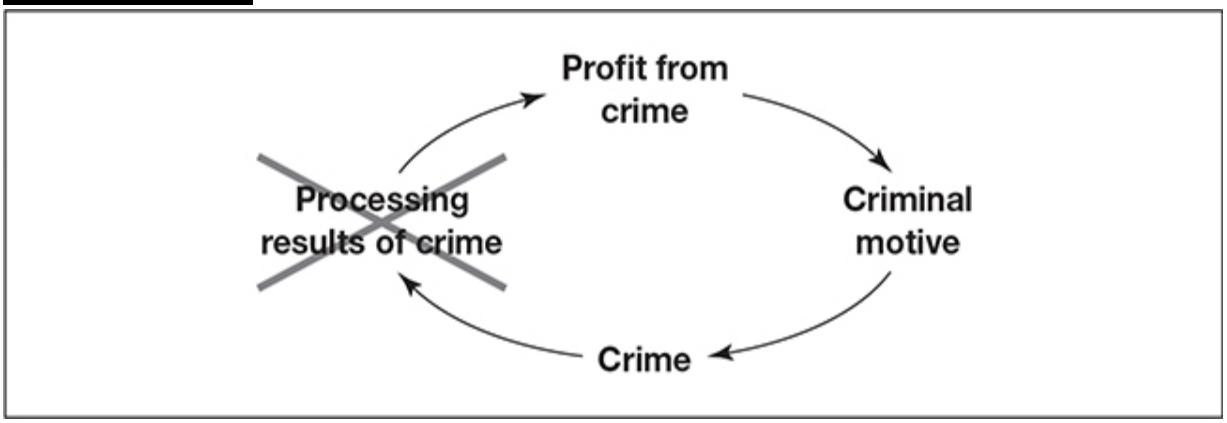
MODERN STRUCTURES OF ORGANISED CRIME AND TERRORISM

As was seen in Chapter 1, organised crime is growing and exerting an increasing effect on the world and its societies. Between USD 3 and 4 trillion each year is estimated to be laundered through the world's financial system, much of it controlled by organised criminal enterprises, some of which are better known than others. Having this kind of money allows criminal groups not just to enjoy luxurious work-free lifestyles, but to subvert international agendas, bribe corrupt politicians and government officials to pass laws which protect them and allow them to expand their criminal activities unchecked by law enforcement. If left unrestricted, such

criminal groups could control entire countries and regions, destabilise world markets and strike lucrative deals with terrorist groups to permit training and organisation on their territory and provide sanctuary.

The battle against money laundering as it is played out within the financial community rests upon the theory of interdiction. Throughout history, and into the future, profit motivates criminal activity. This is represented in Figure 7.1. But the amount of profit produced by criminal activity these days is so large that an additional stage needs to be added for criminal organisations, which is the processing of the profits from crime. Modern international anti-money laundering strategy is predicated upon the assumption that if you can disrupt the processing of criminal proceeds – effectively interdicting them within the global financial system – then you can disrupt this 'magic circle' of causation.

Figure 7.1 **The circle of criminal causation**

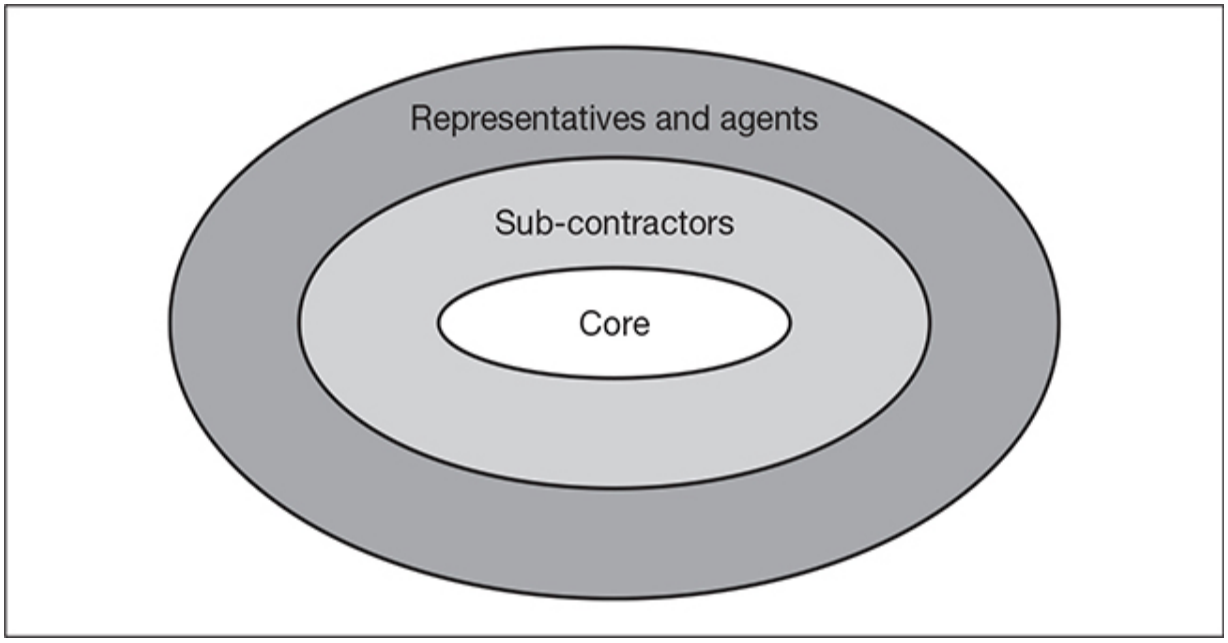


Clearly such a strategy will never result in the elimination of crime. Rather, it is aimed at reducing the flow of criminal funds and trying to ensure that criminal activity should be made as risky as possible for those minded to undertake it, with no degree of profit certainty at the end of it.

Modern TNOC has several features that make it distinctive from more traditional stereotypes. Modern transnational criminal groups will not organise according to traditional, hierarchical structures (compared with the rigid family hierarchies of the mafia type organisations, for example). This makes them harder to predict and penetrate. They are, rather, network

based, using specialists on a 'one job only' basis (much the same as contracting firms may use sub-contractors only for specific, finite work).
For example, a modern TNOC syndicate might use different resources for importation of goods; transportation of those goods in-country; fraudulent documentation to legitimise the presence of goods in a particular country; street enforcement; and money laundering. This lack of formal structure and rapid appearance and disappearance of different combinations makes the organisation more secure. It also makes it more efficient; there is less scope for 'gang politics', with the organisation being purely profit driven and completely ruthless in the pursuit of its objectives.
According to this model of TNOC (see Figure 7.2) , the global financial system is especially vulnerable to abuse because of the use of a wide range of professionals and others with traditionally easy access to the financial system, as fronts for introductions and the conduct of financial and business transactions. Examples of these representatives and agents are well known, but include:

Figure 7.2 **Model of transnational organised crime**



- lawyers
- accountants

- financial advisers
- bankers
- stockbrokers
- IT specialists
- business people
- politicians
- civil servants (judges, magistrates, police officers, customs, military personnel)
- compliant media professionals and public relations specialists
- clerics.

In relation to terrorism, after the collapse of the socialist world, the spread of 'new' terrorism, different in form from 'old' traditional terrorism, has taken place. New ideologies, new factors and new sponsors have entered terrorism, and 'new' terrorism is arguably much more difficult to deal with than 'old' terrorism. 'Old' terrorism was 'political': it was all about achieving concrete political aims and tasks. It supported left wing ideologies such as Marxism and Maoism, and also nationalism and separatism. 'Old' terrorists were invariably ready to negotiate: they promised to stop terrorist action in exchange for concrete political compromises and, for the most part, they did not feel any particular affiliation with religion. Indeed, religious figures of all denominations often condemned them and their actions.

Old terrorism still exists and its most recent high-profile exponents have probably been the LTTE (or Tamil Tigers) in Sri Lanka (who, despite their apparent military defeat in 2010, may yet re-emerge as a coherent force). However, it has been superseded in recent years by the rise of 'new' terrorism, most notably stemming from the Islamic world, but also, it is important to note, from many other areas.

A feature of 'new' terrorism is that it often appears to possess no concrete, achievable political goals. Its goal is to destroy modern societies and much of humankind in the process. It uses the concept of the 'asymmetrical threat', at the heart of which lies the doctrine of the superiority of the attackers against their target *at the specific location of the attack*, despite the terrorists' relative weakness against the target overall. Its focus is on the design and execution of indiscriminate attacks to spread panic and make life unlivable, or at least to cause people to question their own lives

and views and those of their governments, whether elected or unelected. Eventually, it has to be assumed that Weapons of Mass Destruction (WMD) may be accessed and used thereby allowing a very small terrorist organisation to mount an attack that causes destruction that is totally disproportionate to its numbers.

In the US as an example, besides the radicalised Islamist groups known to be operating or attempting to operate, groups and movements such as the Animal Liberation Front, the Earth Liberation Front, the Nation of Islam, the neo-Nazis and skinheads of the 'Aryan Front', the World Church of Creator, the National Alliance and, of course the Ku Klux Klan (KKK) have all engaged in terror attacks.

Many serious terrorist groups are evolving new organisational structures that are harder to detect and infiltrate. These groups are often a collection of factions with common interests which form, change and regroup in response to a specific agenda or planned actions. The groups ally themselves according to religious, ethnic or ideological affinities – often based on major grievances against the US or against a perceived 'takeover of the world by Islam'. They are not controlled or directed by any overall 'director of operations'. Instead they tend to be autonomous or semi--autonomous, while being 'inspired' by an organised group in their planning and decision-making functions. The large number of these groups and, in some cases, individuals (often referred to as 'lone wolves'), as well as their lack of central direction and changing organisational structures and affiliations, makes them very difficult to track and interdict.

As they have become more violent, terrorist groups have also expanded the range of targets they consider to be legitimate. As long ago as 1996, Brian Jenkins, senior adviser to the President at the RAND Corporation and an internationally recognised expert on terrorism, noted three potential reasons for this trend:

- First, as generational replacement has occurred within terrorist organisations and their affiliates new leaders have become less concerned with ideological constraints and adverse public opinion.
- Second, in the media age the new leaders desire above all to maintain media attention, and to receive attention they have escalated their levels of violence and used bolder, more shocking tactics.

- Finally, the international dynamics of terrorist groups require that the organisation should demonstrate to its members that it is moving inexorably towards its goals. Increasingly violent tactics generate the impression among members and supporters that things are heading in the right direction.

MECHANISMS AND TOOLS OF INTERNATIONAL COOPERATION

The UN Convention Against Trans-National Organised Crime, 2000 (the Palermo Convention)

The Palermo Convention is currently the main international treaty detailing the obligations of signatory countries to combat cross-border organised crime. Articles 5, 6, 8 and 23 of the Convention identify four offences, which states are required to criminalise, these being:

- participation in an organised criminal group
- laundering the proceeds of crime
- corruption, and
- obstruction of justice.

A serious crime is defined in Article 2 of the Convention as, ‘an offence punishable by a maximum deprivation of liberty of at least four years or a more serious penalty’.
Article 3 defines the scope of the Convention as addressing such crimes ‘where the offence is transnational in nature and involves an organized criminal group’, and goes on to explain that an offence is transnational in nature if it is committed:

(a) in more than one state
(b) in one state but a substantial part of its preparation, planning, direction or control takes places in another state

(c) in one state but involves an organised criminal group that engages in criminal activities in more than one state, or
(d) in one state but it has substantial effects in another state.

An organised criminal group is defined in Article 2 as 'a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences . . . in order to obtain, directly or indirectly, a financial or other material benefit'. Examples of such crimes would include:

- drug trafficking
- money laundering
- trafficking in women and children
- trafficking in illegal fire arms
- smuggling of alcohol, cigarettes and higher-value goods
- illegal immigration
- protection racketeering
- intellectual property piracy
- corruption
- terrorism
- proliferation of WMD.

The Palermo Convention describes certain core areas where international co-operation is required:

- cooperation with international requests for assistance in the confiscation and repatriation of criminal assets
- extradition, and
- mutual legal assistance.

Extradition

Historically, extradition (from *extradere*, meaning the forceful return of a person to their sovereign) was sought for political opponents not common criminals. The earliest recorded extradition treaty dates back to 1280 BC in Ancient Egypt. By the mid-19th century, however, countries were becoming concerned to fight crime and preserve social interests, with the growing acceptance within public international law that countries should either 'extradite or punish'. In other words, if a criminal from another country was

on your territory, you should either punish that person yourselves or extradite them back to their own country for them to be punished there.
This general obligation, however, has become considered insufficient and accordingly has been replaced by treaty obligations, either bilateral (between two states and applicable to no other states) or multi-lateral (applying to lots of states by international agreement). Because of the sensitivities of extradition (see above), the principle of a 'speciality' also features. This means that a state must only prosecute a person for the offence in respect of which they were extradited (this, presumably, to prevent 'political prosecutions' becoming embedded within the extradition system).

Mutual legal assistance

This is also required under the Convention (subject to exceptions, see below) and includes providing assistance to other states in the following areas:

- taking evidence or statements
- effecting service of judicial documents
- search, seizure and freezing of assets
- examining objects and sites
- provision of information, evidence and expert evaluations
- asset tracing and 'any other type of assistance not contrary to . . . domestic law . . . '
- joint investigations and the use of 'special investigative techniques' (e.g. surveillance, electronic listening, phone tapping, controlled delivery, etc.)
- transfer of criminal proceedings from one State Party to another
- transfer of prisoners serving custodial sentences in one country, for the purpose of giving witness evidence in another country
- facilitation and admission of video evidence of witnesses unwilling or unable to travel to the country of the proceedings.

Mutual legal assistance may be refused in the following circumstances:

- if the request does not conform with the provisions of the Palermo Convention

- if the request 'is likely to prejudice the sovereignty, security, public order or other essential interests. . . ' of the requested State Party
- if domestic law would prohibit the action requested
- interestingly, State Parties may *not* refuse requests on the *sole* ground that the offence is also considered to involve fiscal (tax) matters.

INTERNATIONAL COOPERATIVE BODIES

In the Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) arena, there are a number of important bodies that exist to promote international cooperation, as follows.

The Financial Action Task Force (FATF)

This is the international body set up by the OECD countries in 1989 to promote good anti-money laundering practice around the world, described earlier.

International Cooperation Review Group and its predecessor the Non-Cooperative Countries and Territories (NCCT) List

In 2000, FATF took perhaps its most dramatic new initiative to 'name and shame' what it designated as 'Non-Cooperative Countries and Territories' (NCCTs). These were jurisdictions not participating in the general move towards stricter financial regulation and greater international cooperation and which were instead offering financial services under strict banking secrecy and without sufficient control or regulation by the authorities.
The NCCT initiative proved a successful one – at least in getting countries to address the issues through legislation and infrastructure. Of the 47 - countries whose systems were initially reviewed by the FATF in 2000 and 2001, a total of 23 countries were listed as NCCTs. By 2000 the number had reduced to 15 and by 2001 the list was down to just eight countries. By the end of 2007 the list was empty, because all of the designated countries

took steps deemed sufficient to get themselves removed, and passed AML and CFT laws.
If there was one criticism of the NCCT regime, it was that it was a very blunt instrument; it made no distinction between different severities of deficiency and you were either on the list or you were not. It was therefore replaced in 2007 by the International Cooperation Review Group (ICRG), which aims to be less 'black and white' in how it describes the world, instead attempting to engage in a dialogue with countries to improve their AML and CFT regimes, while also publicising those countries where it believes that varying degrees of problems still exist. It currently has three levels of sensitivity, being countries which the FATF has urged should be subject to a call for countermeasures, countries subject to a call to consider the risks of transactions involving them, and countries which have made progress, but where strategic deficiencies still remain to be addressed in their AML regimes.

Moneyval

This is the body set up by the council of Europe in 1997 for the mutual evaluation of members states' AML and CFT measures for Council of Europe and Member States which are not members of FATF.
Along with FATF it is influential in applying peer pressure to countries to get their AML and CFT regimes up to International Standards.

Interpol

This is the international criminal police organisation. It has 190 member countries and was created in 1923. It facilitates cross-border police cooperation and supports and assists all organisations, authorities and services whose mission is to prevent or combat international crime.

The Egmont Group

This is the coordinating body for financial intelligence units worldwide. It was formed in 1995 to promote and enhance international cooperation in AML and CFT (see Chapter 2).

8

Modern Money Laundering and Terrorist Financing: Two Case Studies

Introduction

Smoke and Mirrors: AlnaBank and the Messengers of God

Futura Capital Partners: Modern Money Laundering through ‘low risk’ regulated OECD Financial Institutions

Discussion Points: Futura Capital Partners Case

INTRODUCTION

The two fictional case studies in this chapter provide an in-depth opportunity to consider some of the main issues discussed in this book in a practical, work-based context. Both have been researched and carefully scripted to reflect the day-to-day challenges which arise in trying to make AML policies work amid the pressures of modern business.

Smoke and Mirrors tells a story of global financial institution AlnaBank's relationship with a Cypriot investment firm, J Dalea Investments and, through Dalea, its unwitting exposure to political corruption, organised crime and terrorist groups in the near Eastern country of Moldachia and beyond. (For a video version of this case study email training@lessonslearned.co.uk)

The Futura Group looks at how criminals and money launderers may use a relatively sophisticated knowledge of international AML standards and standard countermeasures to hide criminal funds inside a financial institution operating in a well-regulated, economically developed country.

SMOKE AND MIRRORS: ALNABANK AND THE MESSENGERS OF GOD

Organisational context and operation of the risk-based approach

After the great financial crisis of 2008/09, in which AlnaBank suffered heavy losses and had to take government bail-out money, it sets its sights firmly on renewal and a revival of profitability and

shareholder value. As the crisis recedes and growth returns, Alna's risk focus is very much on those operational risks which were the cause of the crisis, not on money laundering. This 'de-emphasis' of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) risk in relation to other risks is encouraged in part by the adoption of a new, systematic and very process-driven method for managing AML risk, known as the risk-based approach.

Under the risk-based approach, all a bank like Alna has to do to manage its AML risks effectively is to assess its clients before taking them on as either higher or lower risk according to a number of set criteria (country of residence/incorporation/regulation, business type, transaction type/volume, etc.), and thereafter adjust the level of due diligence and monitoring according to the perceived level of risk: enhanced due diligence and monitoring for higher-risk accounts and standard or lower due diligence for lower-risk accounts.

Leading AlnaBank's drive for revenue and growth is the Global Relationships Division (GRD), which is aggressively seeking new business opportunities and is therefore very interested when approached by a Cypriot investment firm called J Dalea Investments that is interested in placing initially €1 billion with GRD for management.

Relationship origination, reliance and the AML governance structure

Because of the importance attached by AlnaBank to customer due diligence (CDD), a special unit has been formed in GRD called the Business Unit Support (BUS) group to assist the Relationship

Managers (RMs) with obtaining all the documents and verifications required under AlnaBank's group AML policy – particularly for higher-risk accounts where the CDD burden is greatest. What develops under this arrangement, however, is a 'disconnect' between the RMs on the one hand, who see their role very much as revenue earners for the bank and who generally believe that the CDD process has become too complex and time-consuming, and the BUS team members on the other hand, who believe that the RMs don't take CDD seriously enough . . .

This division comes to a head over the Dalea Investments account. Under AlnaBank's own policy and also under international standards, where a financial intermediary client is being taken on, who in turn has its own clients on its books, it is acceptable to rely on the CDD conducted against those end clients by the intermediary itself, as long as the intermediary agrees to such reliance and as long as it is incorporated and regulated in an 'equivalent jurisdiction' (which Dalea Investments, incorporated in Cyprus, an EU country, is). The personnel in GRD, right up to its Group Executive Director, Daniel Johnson, believe that this is sufficient and don't wish to undertake further due diligence against Dalea's own clients if it isn't necessary. The BUS personnel, however, consider that further due diligence is not only justified but necessary, given the fact that Dalea Investments is relatively unknown, that the sums involved are so large and given also that the jurisdiction in question (Cyprus) has in the past been associated with inflows of money from high-risk jurisdictions, such as countries of the former Soviet Union.

The issue goes for a decision to the most senior level within the bank and results in a corporate decision, communicated by the Chief

Executive, Greg Jonas, that further due diligence will need to be undertaken against Dalea Investments' own clients. The communication from Jonas, however, makes it clear that he expects BUS to be aware of the very demanding revenue targets that the bank is pursuing and to work with the business 'as a team' to help achieve those targets.

Further due diligence and client acceptance

BUS therefore conducts further, deeper due diligence against Dalea Investments' own clients by accessing Dalea's own CDD records, which reveal that the main client is a group of companies based in the former Soviet Republic of Moldachia, with an extremely complex corporate structure consisting of multiple layers of shell and holding companies. Nevertheless, it appears that Dalea Investments has done its due diligence against this structure, as required, and what it reveals is that the ultimate beneficial owner of the Xavier Group is a local lawyer and businessman by the name of Yulian Garbov. One unresolved issue is a rumour (no more than that) in Moldachia that apparently Yulian Garbov is a 'front' for an unnamed Moldachian politician. But Dalea Investments' due diligence reveals nothing on that, and despite the fact that the BUS group want to conduct further, deeper investigations into this allegation, it is also mindful of how much time has already been spent on due diligence and, under strong business pressure, the Head of Compliance, Ottily Marks, agrees to the opening of investment accounts for Dalea Investments. She stipulates that although Garbov himself is not technically a Politically Exposed Person (PEP) under the bank's policy, nevertheless he poses similar risks and should be

treated as such, that the account should be the subject of regular, enhanced monitoring and that the Head of GRD, Daniel Johnson, should sign off on the account. In fact, Johnson never does sign off on the account.

When the account is opened, €3 billion is received instead of the €1 billion initially promised. Furthermore, a correspondent bank account relationship is opened in AlnaBank's New York office one year later with KVP Bank, a wholly owned subsidiary of the Xavier Group, based substantially on the existing due diligence against Xavier Group.

The real position: PEP ownership, political corruption, organised crime and terrorism

Following a revolution in Moldachia, details emerge of the extent of corruption in the previous government, particularly by the former Minister of Transport, Vassiliy Chernov, who had been accepting large political donations from a Moldachian businessman named Radovan Kaltan, who was also rumoured to be the ultimate controller of the main Moldachian organised criminal group. Aware, now, of Kaltan's political donations to Chernov, and aware also of the rumour that Yulian Garbov was not, in fact, the ultimate beneficial owner and controller of the Xavier Group, Moldachian journalist Judi Shimanova suspects that Vassiliy Chernov has been the true owner and controller of Xavier Group all along and that he has allowed Kaltan to launder criminal funds through it in return for his donations.

Using information from ex-employees of Xavier Group, Judi Shimanova discovers hundreds of millions of dollars' worth of

apparently fake transactions between companies in the Xavier and Kaltan groups, involving large payments against invoices issued for items that are difficult to physically trace and assess, such as consultancy services, intellectual property rights on designs, outsourcing services, etc. What nobody has previously been aware of, however, is that Radovan Kaltan has been secretly cooperating with an Islamist terror group known as the Messengers of God that provides security for his illegal gambling, prostitution and alcohol operations in neighbouring Maluchistan in return for the use of some of Kaltan's companies for terrorist financing purposes. As part of these transactions, funds originating in Iran have made their way through Kaltan-controlled shell companies to the Xavier Group pocket bank, KVP Bank, which now of course has correspondent banking relationships with AlnaBank in New York . . .

In the US, investigators uncover a plot by the Messengers of God to use some of these funds to explode a dirty bomb in downtown Manhattan.

Questions on due diligence deficiencies and failures

At the time of account opening, what did AlnaBank do, or fail to do, that exposed it to the risk of money laundering and terrorist financing?

The failures were notable and extreme, but perhaps not unpredictable, given the extreme performance pressure which business units of the bank were under and the failure of the governance structure (see below).

Risk assessment

Those involved failed to assess the risks of the relationship with Dalea Investments correctly. Particularly on the business side, the assumption was that as long as Dalea came from within the EU, it could effectively be treated as ‘low risk’, which isn’t necessarily the case. Factors such as the size and reputation of the intermediary in question and the recent financial and economic history of the jurisdiction should all be taken into account.

Depth of due diligence

Even though the above point was eventually accepted, the acceptance seemed to be reluctant and almost certainly influenced the depth of the further due diligence undertaken. AlnaBank seemed to satisfy itself with simply checking the due diligence records which had been obtained by Dalea Investments and failed to conduct its own investigations. The minimum requirements in terms of paper documentation, certificates of incorporation, passport copies, etc. seemed to be there. There was also evidence from corporate reports and local newspapers that Xavier Group was a genuine business. What was missing, however, was any real investigation into Xavier Group’s business, its source of wealth (i.e. what produced its revenues) and its business counterparties and trading partners. The journalist Judi Shimanova started asking these questions and quickly got answers. Why didn’t AlnaBank? Was it really not possible for it to discover the business connections between Xavier Group and companies controlled by Radovan Kaltan? And was there really no way in which they could have discovered Kaltan’s dubious reputation within the country? Likewise, even though Dalea Investments claimed to have reached a

dead-end in determining the ‘rumour’ that Yulian Garbov, the supposed ultimate beneficial owner of Xavier Group, was connected to an unnamed senior political figure, AlnaBank again made no attempt to get to the bottom of the matter. Had it done so, the connections with the Minister of Transport, Vassiliy Chernov, may have been detected.

Failure to conduct proper due diligence against a correspondent bank

After the Dalea Investment accounts were opened, a correspondent banking relationship was set up between AlnaBank’s New York office and a wholly-owned banking subsidiary of the Xavier Group called KVP Bank. The due diligence relied upon for that account was the same flawed due diligence in existence for the Xavier Group. In other words, the bank assumed that because the Xavier Group had been deemed acceptable, then any subsidiary – including a banking subsidiary – would also be acceptable. Alna took none of the required CDD steps referred to below against its new respondent, KVP Bank. Had it done so, that would have provided another route for the discovery of Xavier Group’s connections with Kaltan-controlled companies.

What do international standards and well-drafted procedures and controls require in relation to customer due diligence?

FATF Recommendation 10 sets out that financial institutions must conduct due diligence against entities with which they form business relationships. ‘Due diligence’ means:

- establishing and verifying the identity of the person or entity concerned
- establishing the beneficial ownership of the asset concerned – meaning the natural person who owns or controls the asset, or on whose behalf transactions are being conducted
- establishing the purpose of the business relationship; and
- conducting ongoing monitoring to ensure that transactions are consistent with what is known about the customer.

It also states that due diligence should be conducted on a risk-sensitive basis and Recommendations 12 and 13 go on to state that in relation to higher-risk relationships involving PEPs and cross-border correspondent banking relationships, additional measures should be taken.

In relation to PEPs, these measures are:

- developing risk management systems to determine whether the customer or the beneficial owner is a PEP
- obtaining senior management approval for the commencement of the relationship
- taking reasonable measures to establish the PEP's source of wealth (that is, the economic activity that has generated their wealth) and source of funds; and
- subjecting the relationship to enhanced, ongoing monitoring

In relation to cross-border correspondent banking, the additional measures are:

- assessing the correspondent bank's business and customer base
- assessing the strength or otherwise of its AML/CFT controls, the quality of its supervision and whether it has been the subject of investigation or regulatory action
- documenting the responsibilities of each institution
- obtaining senior management approval for the commencement of the correspondent banking relationship; and
- ensuring that where the respondent bank's (i.e. KVP Bank's) own customers will be accessing its accounts with its correspondent bank (i.e. AlnaBank), the respondent bank has identified its own customers and can and will provide CDD records in relation to them upon request.

In practical terms, a bank's policies and procedures would require extensive due diligence against a corporate group such as the Xavier Group and its subsidiary bank, KVP Bank. The complex corporate structure would need to be unwrapped and understood, and also the *reason* for the complexity of that structure. Natural persons owning 25 per cent or more of the shares or voting rights in the corporations in question would need to be identified, and their sources of wealth established. In particular, investigations would need to be undertaken into the business activities of the corporate group, how it made its money, who its trading partners were, the type and amount of transactions which it conducted, and also its status and reputation within the country – not just from local newspapers but also from multiple, independent, unbiased sources. Some banks would employ the services of professional investigations consultancies in these

circumstances, with access to a wide range of sources and contacts both public and non-public.

Due diligence investigations in high-risk situations such as this, whether they are in respect of individuals (e.g. Garbov) or corporate groups such as the Xavier Group, need to be thorough and detailed and supporting evidence needs to be obtained and retained on the file.

Questions on beneficial ownership and PEPs

What mechanisms were used by those involved to disguise beneficial ownership and political connections?

Use of fronts

The former Minister of Transport, Vassiliy Chernov, used the lawyer and businessman Yulian Garbov as a 'front' to disguise his own ownership and control of the Xavier Group. The use of fronts in this way is very common and is extremely difficult to detect, because there will usually be no formal record or document confirming the controller's interest (that, after all, is the whole point). When fronts are used, the true controller's name doesn't appear anywhere in the documentation relating to the account, trust or company concerned. When a suspicion exists, therefore, that a front may be being used, one is often left with less than satisfactory indicators. These include:

- the credibility of the suspected front
- the extent and credibility of market rumours and information about whether a relationship between the suspected front and suspected controller does in fact exist, and if so its nature and extent

- careful and detailed searches through public records using not only subscription products such as World-Check but also general search engines such as Google, searches in online international, regional and national newspapers (although these can be suspect – see below) and other information sources such as society magazines and informal conversations with other banks, companies and professional firms such as lawyers and accountants.

In addition, there is personal questioning – often referred to as 'the smell test'. A succession of meetings at which a range of important and detailed questions are asked over a period of time can assist in developing an accurate impression. A person's demeanour, the confidence with which they speak, the extent of their knowledge and mastery of the relevant issues, whether they change their minds on important issues without apparent reason, whether they give different answers to the same questions asked (deliberately) at different times during the process, are all matters which can be taken into account.

Ultimately, it is extremely hard to spot a controller–front relationship if it has been carefully constructed. The important thing is that a bank should be able to show that it has gone through a structured – and not necessarily easy or trouble-free – process to arrive at a decision. Nobody can ask that you get it right all the time, but they can – and do – ask that you make a reasonable and genuine attempt at finding out. Simply saying 'It's a rumour, maybe it's true, maybe it isn't' won't suffice.

Complex structures

Complex structures can develop for legitimate reasons, such as during and after a series of corporate acquisitions when there has been no opportunity to simplify the corporate structure. But they also have a more sinister use in that they are an ideal mechanism for hiding ownership. The more complex a corporate structure is in terms of the number of companies, the ownership layers and the degree of inter-company ownership, the harder it is to determine the natural persons who are actually in control.

A bank should adopt a clear policy that unless the reason for it is clearly understood, any corporate structure at or above a certain number of layers of ownership (e.g. three or four) should automatically be designated as a higher-risk account and therefore subject to enhanced due diligence and enhanced ongoing monitoring. Enhanced due diligence in these circumstances would entail peeling back the corporate structure (something which can take many weeks or even months) so as to fully understand it and determine the identity of the natural persons holding 25 per cent or more of the shares or voting rights or who otherwise appear to be individuals who are exercising significant influence over the affairs of the company/structure concerned.

During this process, the investigations themselves and the conversations that are had with officials and managers of the company can often assist in developing a sense of whether or not it would be appropriate to proceed. Ultimately, if, at the end of the process, one simply isn't satisfied that the true beneficial ownership of a complex structure has been established, then the business should either be refused or requirements expressed as to the level of

transparency and restructuring which would be necessary in order for the Bank to proceed.

Public disinformation

People wishing to hide their control over a company or its assets are fully aware that banks these days will look to a wide variety of sources of information in trying to establish true beneficial ownership, and are often prepared to disseminate false or deliberately misleading information in order to improve perceptions about themselves. The purpose of this may be either to help persuade you that a rumour of a connection isn't true, or to enhance the credibility of a front as a genuine owner/controller. Articles in newspapers, journals and websites, internet blogs, even official announcements from government bodies (where these have been corrupted) mingle with other information and are, to all extents and purposes, indistinguishable. In such circumstances, the quality of the information obtained – and in particular an assessment of the quality of the source of that information – becomes paramount and this is an area where many financial institutions again turn to professional investigation firms and the specialist services they offer.

Money laundering and terrorist financing

What mechanisms do criminal and terrorist groups use to move money around and launder it?

Money laundering

Radovan Kaltan was apparently laundering the proceeds of his Moldachian criminal activities out of the country and into Cyprus by

getting shell companies which he owned and controlled to engage in apparently legitimate business transactions with Xavier Group companies. These funds would then be transferred to the ‘pension fund’ and onward to Dalea and AlnaBank.

While some of these trading transactions were no doubt genuine, others will either have been completely fabricated or substantially over- or understated, and will have involved tactics such as false invoicing, over-invoicing and under-invoicing.

For example, a false invoice for a fake transaction from an Xavier company to a Kaltan company would provide an apparently legitimate business purpose for the transmission of funds from the Kaltan company to the Xavier company, then to be fed on out via the pension fund to Dalea Investments in Cyprus and thence on to AlnaBank. Laundered funds coming back the other way could be transferred back to other Kaltan companies under cover of similar invoices issued by those companies to Xavier companies.

The process therefore involves the laundering of criminal funds in a sophisticated scheme involving genuine companies and shell companies, genuine transactions and fake transactions, a corrupt politician, his ‘front’ and the business structure beneath him, a regulated financial intermediary and an international financial institution. Through this network, the criminal provenance of some of the funds in the AlnaBank accounts is hidden from view. AlnaBank sees initially only Dalea, and subsequently the Xavier Group and Yulian Garbov. It doesn’t see behind them Vassiliy Chernov, Radovan Kaltan or the Messengers of God (see below).

Terrorist financing

The terrorist financing undertaken by the Messengers of God utilises many of the money laundering features outlined above, in particular, the use of shell and front companies as cover for the transfer of funds.

The added element in the case is the use of the Xavier Group pocket bank, KVP Bank. (A 'pocket bank' is a bank owned and controlled by a particular corporate group, or sometimes even a particular individual, and which often has only one customer, or a relatively small number of customers who are associated with the group or the individual.) Following the transmission of funds from Iranian shell companies to the accounts of the Kaltan-controlled companies with KVP Bank in Moldachia, the funds are then wired to KVP Bank's dollar clearing account with AlnaBank in New York, for onward transmission, presumably to other companies and individuals inside the US. By this method, the Messengers of God would make funds available to its accomplices inside the US for its purposes there; much the same as happened with the 9/11 attacks, only on a larger scale due to its (expensive) ambition of exploding a dirty bomb in downtown Manhattan.

Criminal groups and terrorist groups will sometimes cooperate when it is expedient to do so. The most high-profile example of this in recent years was the cooperation between the Taliban (pre-2001) and those engaged in drug trafficking from the poppy fields of Afghanistan, which suited the needs of both groups. The Taliban were able to finance their regime and the drug lords were able to continue with their lucrative, illicit trade.

What does the law require you to do if you become suspicious of money laundering or terrorist financing?

You *must report* suspicions of money laundering or terrorist financing *immediately* to your Compliance Officer or Money Laundering Reporting Officer, who will advise you further on what is required.

Failure to report a suspicion and/or warning or 'tipping off' a customer that a report has been filed and that they may become the subject of an investigation are *serious criminal offences* in almost all jurisdictions.

If you are in any doubt at all, speak to your Compliance Officer or Money Laundering Reporting Officer.

Questions on organisational responsibilities for CDD

In what way or ways did AlnaBank's AML/CFT governance structures fail it in this case?

The division between business-getters and business-controllers

While the division of responsibilities in AlnaBank between the RMs and the BUS group made sense in theory – and is indeed a model followed in many financial institutions – in practice it didn't work out. The RMs came to the conclusion that the BUS group was simply there to stop them doing business (as evidenced by the acronym they attached to the 'New Client Acceptance' system or NCA – 'No Clients Any More'). The BUS group clearly came to the conclusion that the RMs wanted any kind of business, regardless of risk. Thus, the two parts of the bank were fighting each other instead of cooperating towards a common goal.

Senior management contribution

The main players involved fell well short of their responsibilities. The business head, Daniel Johnson, was too focused on the GRD's revenue targets and on the contribution which the Dalea business would make to them – preferably at minimal cost – to appreciate the wider risk implications of AlnaBank getting involved in that business. As part of the GRD business structure, the BUS group would have felt completely undermined by what was happening.

For her part, the Head of Compliance, Ottily Marks, and her Compliance team whose role was to support the BUS group from outside of business reporting lines, had clearly failed to make the case for effective CDD to the business team in GRD, which indicates a failure in the training and communication strategy. While a degree of awareness and sensitivity to other people's positions is always required, her most serious mistake was in agreeing to allow the accounts to be opened when both she herself and those on the BUS team who had been working on the case in detail were fundamentally dissatisfied with the extent of the due diligence which they had reviewed from Dalea. Thereafter they failed to follow up on the enhanced monitoring and relationship sign-off that Daniel Johnson should have executed, which she had stipulated was necessary in her account opening approval email. Had monitoring taken place, it is possible that warnings would have been raised and suspicious activity reports filed in relation to the receipt of *three times* the expected funds from Dalea (€3 billion instead of €1 billion).

The Group Chief Executive, Greg Jonas, while seemingly supporting the Compliance Department's position that the bank

needed to look behind J Dalea Investments, nevertheless appeared to do so reluctantly and his approval words contained a barely disguised warning that Compliance and the BUS group within GRD would be expected to display a little more understanding in future. This was probably influential in Marks' later decision not to push for further, extensive due diligence on the rumour about Garbov's political connections and on the real nature of Xavier Group's business activities in Moldachia.

What might individual senior managers appearing in the case have done differently?

Daniel Johnson, Head of GRD

He could and should have insisted that CDD be done properly. As a senior business leader, Johnson should have been aware that it was he and his business that was primarily responsible for customer due diligence and that scrimping and saving on it in terms of time and money is a false economy, especially when dealing with relationships which are not 'plain vanilla' low risk, which was definitely the case with the Dalea Investments relationship.

If Johnson had problems with the way in which the BUS group was doing its job, instead of expressing this in the form of tactical fights on specific cases, he could have sought to engage the BUS group and the compliance department in a discussion about how the two could work together for the general benefit of the business.

Ottily Marks, Head of Compliance

Seeing the way things were going, Ottily Marks as the Head of Compliance could and should have sought to address the divisions

between the business and the BUS group in GRD through a programme of training and communication. As part of this programme she could have obtained their views on ways in which the CDD process could be streamlined and made to work more efficiently, while also stressing of course that the fundamental requirements of knowing the customer and establishing beneficial ownership, political connections, etc. would need to remain.

Marks should also have tried to use her powers of persuasion – with both the Head of GRD, Daniel Johnson, and the Group CEO, Greg Jonas – to convince them that the risks of proceeding with the account without undertaking further and more detailed checks in Moldachia, were too great.

Greg Jonas, Chief Executive of AlnaBank Group

He should have been far less equivocal in his communication about the requirement for effective CDD at all times. Instead of planting the seeds of doubt about his support in Ottily Marks' mind with his email, he could instead have insisted that both Johnson and Marks together lead a joint project between GRD, the BUS group and the Compliance Department to review the Bank's CDD policy and procedures as part of a programme to start reducing the unhealthy tension which was contributing to the creation of unacceptable risks for the bank.

FUTURA CAPITAL PARTNERS: MODERN MONEY LAUNDERING THROUGH 'LOW

RISK' REGULATED OECD FINANCIAL INSTITUTIONS

You are a business manager and in that capacity you are assessing the suitability of Futura Capital Partners as a potential counterparty with your firm. Read the information in your groups and then discuss and answer the questions given at each stage. Be prepared to discuss your answers in plenary with the other groups when your facilitator debriefs you. This task is in three parts and your facilitator will let you know how long you have for each part. (For printable versions of this case study email training@lessonslearned.co.uk)

Part 1

1.1 Futura Capital Partners ('Futura') is a successful and rapidly growing Netherlands-based investment management and private equity firm with €500 million of Assets Under Administration (AUA) and is 'an intelligent, thoughtful fund manager and business growth management specialist with a good understanding of risk and a deep, well-honed insight into what makes a successful investment' (*Investment Week)*.

1.2 Futura has been introduced by you, following an approach made to you by one of its owners and directors, an old university friend, Stanley Hardberg, with whom you have kept in touch off-and-on over the years. Futura is based in Amsterdam with six directors and a total of 19 staff housed in modern offices in Weesperstraat. The fund manager is regulated by the AFN (Autoriteit Financiële Markten) and the firm was described by *Investors Chronicle* as 'one of the

Netherlands' most exciting and fastest-growing investment managers and private equity funds – an experienced, capable firm that will seek out the best returns for you, according to your risk appetite'.

1.3 The other director to whom you are talking other than Hardberg is Jost van der Cleef, the Managing Director. Both van der Cleef and Hardberg are Dutch nationals with extensive experience in the financial services industry both in the Netherlands and the rest of Europe. Hardberg worked for Deutsche and Dresdner in Germany and van der Cleef with Citi and Standard Bank of South Africa in London before both moved to ABN Amro, from where they then moved to set up Futura. Corporate information issued by Futura, market analysis of their portfolios and conversations with other market participants indicate that Futura's client base is divided broadly into two sectors. First, they have traditionally attracted investments from high net worth individuals – both personal wealth and corporate funds from their businesses, these relationships having been primarily developed during van der Cleef's and Hardberg's days with their previous employers. Second, however, with the growth of the firm and its positive press coverage in recent years, they have also started to attract big money with pension fund placements from a growing number of Dutch and other European medium-sized businesses, along with a couple of multi-nationals.

1.4 If you decide to proceed, van der Cleef and Hardberg will sign the necessary legal documentation. The other members of

the Futura management board and their responsibilities are shown in Table 8.1.

As a licensed financial institution within an EU country. Futura's AML policy, systems and controls are deemed to be compliant with European and international standards.

Please now discuss and answer the following questions before moving on to the further information provided.

- How would you analyse the risks in this potential intermediary?
- What due diligence would be required?
- Are there any other issues for consideration?

Table 8.1 **Management Board Composition of Futura Capital Partners**

Name	Nationality	Location	Tax Domicile	Title/ Responsibilities
Jost van der Cleef, 45	Dutch	Amsterdam	Netherlands	Managing Director
Stanley Hardberg, 45	Dutch	Amsterdam	Netherlands	Finance Director
Jan van der Kuyt, 38	Dutch	Amsterdam	Netherlands	Director – Business Development, European Corporates
Priscilla van Meerden, 37	Dutch	Amsterdam	Netherlands	Director, Analysis and Research
Roberto di Michele, 64	US	Miami, Florida	United States	Non-Executive Director
Schalk de Klerk, 68	South African	Johannesburg	South Africa	Non-Executive Director

Part 2

Research into Futura reveals the fund and ownership structures depicted in Figure 8.1.

2.1 Due diligence research into Futura reveals the primary legal adviser to be Marcus Trellick, a partner in City of London law firm Hartwell Mason, which also has offices in Amsterdam, Copenhagen and the Netherlands Antilles. He has provided a letter confirming the structure and also legal opinions from the Dutch and Netherlands Antilles offices confirming that the structure's purposes are legitimate and do not offend against relevant tax laws. Upon specific inquiry, Marcus Trellick, in a conference call also confirmed, in addition, that the targeted international shareholder structure

required the offshore location in order to ensure the same tax treatment for all investors. He also explained that any remuneration to the management team, including carried interest, would be channelled through a Dutch Stichting and confirmed that no member of the management team would have any power to directly dispose, alone or jointly, of any assets of the fund's accounts.

2.2 At a meeting with Mr van der Cleef, you ask about the respective roles of the two non-executive directors, Roberto di Michele and Schalk de Klerk. Mr van der Cleef informs you that Roberto di Michele is a former investment banker who moves extensively within circles of wealthy, retired businesspeople in Florida, whose role is to attract investments from these sources. He is at pains to emphasise that the high net worth clients attracted by Mr di Michele are all US citizens (often with eminent backgrounds) based in the United States, and that funds invested with Futura are always sourced from US financial institutions.

Figure 8.1 **Ownership structure of the Futura Group**

Name	Nationality	Location	Tax Domicile	Title/ Responsibilities
Jost van der Cleef, 45	Dutch	Amsterdam	Netherlands	Managing Director
Stanley Hardberg, 45	Dutch	Amsterdam	Netherlands	Finance Director
Jan van der Kuyt, 38	Dutch	Amsterdam	Netherlands	Director – Business Development, European Corporates
Priscilla van Meerden, 37	Dutch	Amsterdam	Netherlands	Director, Analysis and Research
Roberto di Michele, 64	US	Miami, Florida	United States	Non-Executive Director
Schalk de Klerk, 68	South African	Johannesburg	South Africa	Non-Executive Director

2.3 Mr Schalk de Klerk, it emerges, is Mr van der Cleef's father-in-law, who is a wealthy and respected South African businessman. Apparently, many South Africans keep significant assets offshore (i.e. outside South Africa) as a hedge against political risk in that country. Mr Schalk de Klerk's role is to use his contacts and influence to attract these investment funds towards Futura.

2.4 There is a lot of pressure, coming from senior levels in your firm, to get the deal signed up. This is due to the challenging nature of the end-of-year targets, on which significant senior manager bonuses are dependent.

Please discuss and answer the following question:

What effect does this information have on your risk assessment of the potential relationship?

Part 3

As an Operations Team, **YOU HAVE 15 MINUTES** within which to notify the Facilitator of which persons and entities you wish to conduct due diligence checks against. Your Facilitator will then provide you with whatever information he/she has which is relevant to your request.

Note to trainer. Figures 8.2 to 8.7 contain search results that are relevant to the desired further due diligence in this case. Provide copies of each figure only to those teams that have specifically asked for search information pertaining to the individual or entity covered by that particular figure.

Figure 8.2 **Public internet search against Executive Directors**

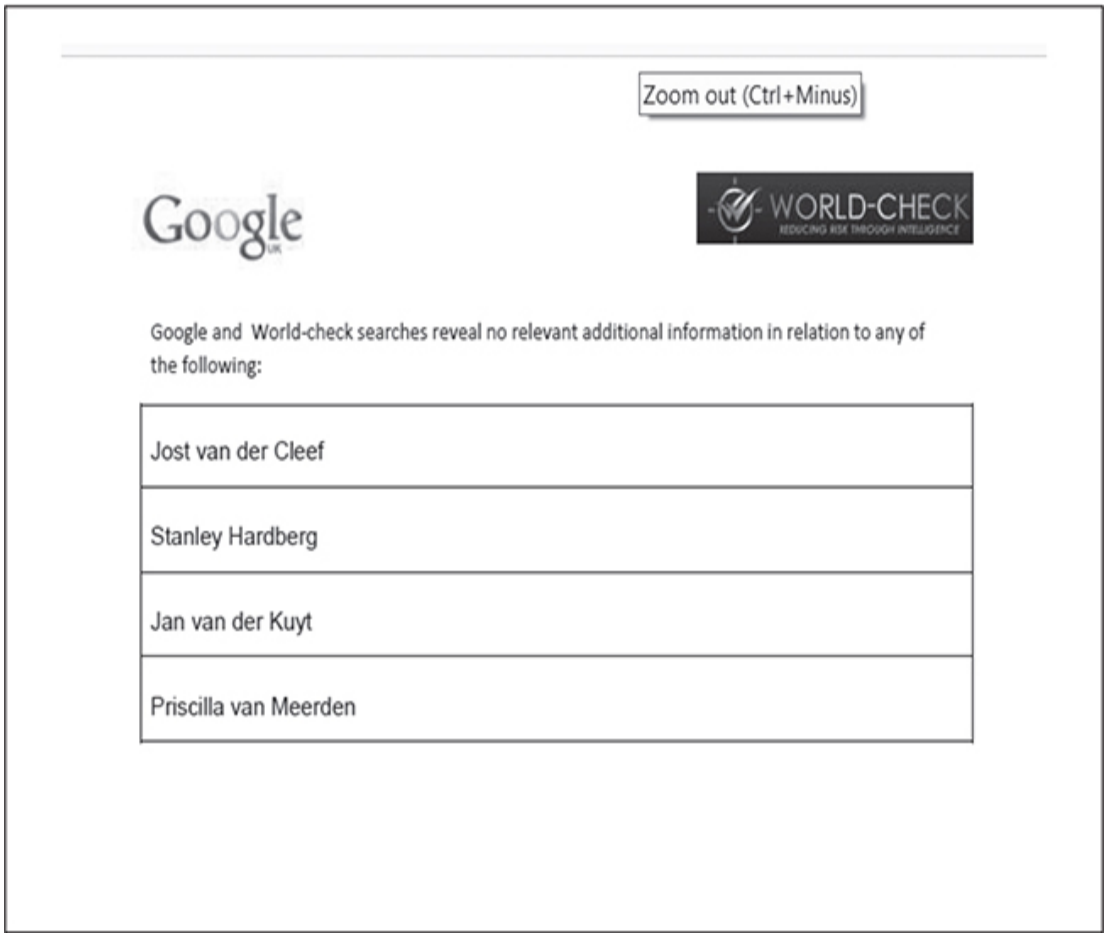

Zoom out (Ctrl+Minus)
Google
WORLD-CHECK
Google and World-check searches reveal no relevant additional information in relation to any of the following:
Jost van der Cleef
Stanley Hardberg
Jan van der Kuyt
Priscilla van Meerden

Figure 8.3 **Public internet search against Non-Executive Directors**

Google

In relation to ROBERTO DE MICHELE , no additional relevant information is available.

In relation to SCHALK DE KLERK, Google points you to a Wikipedia entry as follows.

WIKIPEDIA
The Free Encyclopedia

Article Talk Read Edit View history Search

Schalk de Klerk

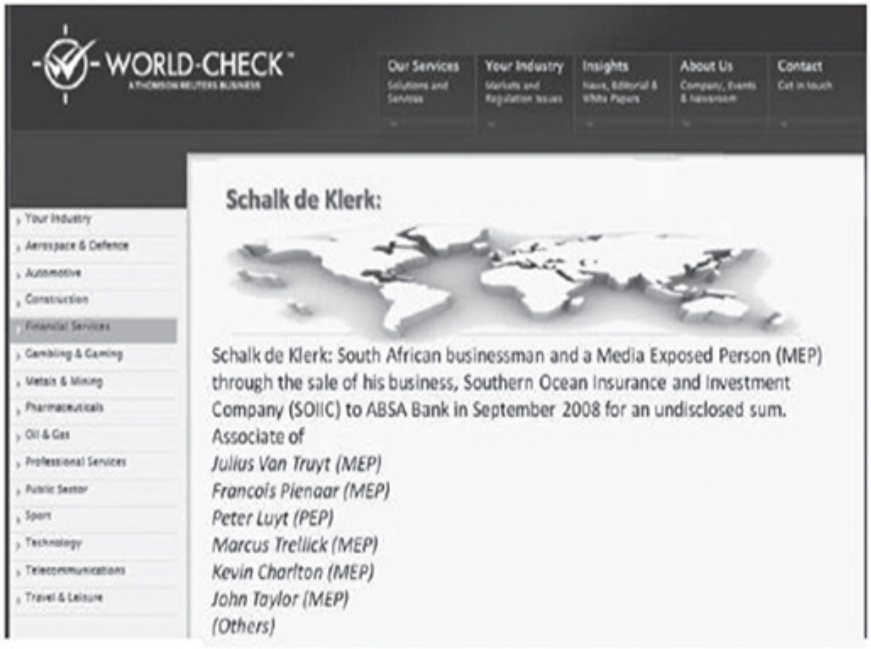
From Wikipedia, the free encyclopedia

For Wikipedia guidelines, see Wikipedia:What's Schalk de Klerk

This article's lead section may not adequately summarize all of its contents. Please consider expanding the lead to provide an accessible overview of all of the article's key points. (June 2010)

Schalk de Klerk is a prominent South African businessman based in Cape Town, Republic of South Africa. In 1972 de Klerk founded The South Ocean Insurance and Investment Company (SOIIC), which he sold to ABSA Bank in 2008 for an undisclosed sum. De Klerk was also active in South African rugby union and between 1995 and 2001 served on the advisory board of the South African Rugby Union.

A Worldcheck search against de Klerk reveals the following pertinent information



WORLD-CHECK
A THOMSON REUTERS BUSINESS

Our Services | Your Industry | Insights | About Us | Contact

Schalk de Klerk:

Schalk de Klerk: South African businessman and a Media Exposed Person (MEP) through the sale of his business, Southern Ocean Insurance and Investment Company (SOIIC) to ABSA Bank in September 2008 for an undisclosed sum.
Associate of
Julius Van Truyt (MEP)
Francois Pienaar (MEP)
Peter Luyt (PEP)
Marcus Trellick (MEP)
Kevin Charlton (MEP)
John Taylor (MEP)
(Others)

Figure 8.4 **Specialist internet search against Marcus Trellick**

Google

In relation to MARCUS TRELLICK , Google points you to a Wikipedia entry as follows.

WIKIPEDIA
The Free Encyclopedia
Article
Talk
Read
Edit
View history
Search
Marcus Trellick
From Wikipedia, the free encyclopedia
This article's lead section may not adequately summarize all of its contents. Please consider expanding the lead to provide an accessible overview of all of the article's key points.
Marcus Trellick is a partner in London law firm Hartwell Mason, where he heads up the firm's non-contentious Investment and Tax practice, advising commercial and private clients on investments, company formations, trusts, tax planning and the use of offshore structures.
(Link to website)

A Worldcheck search against Trellick reveals the following pertinent information

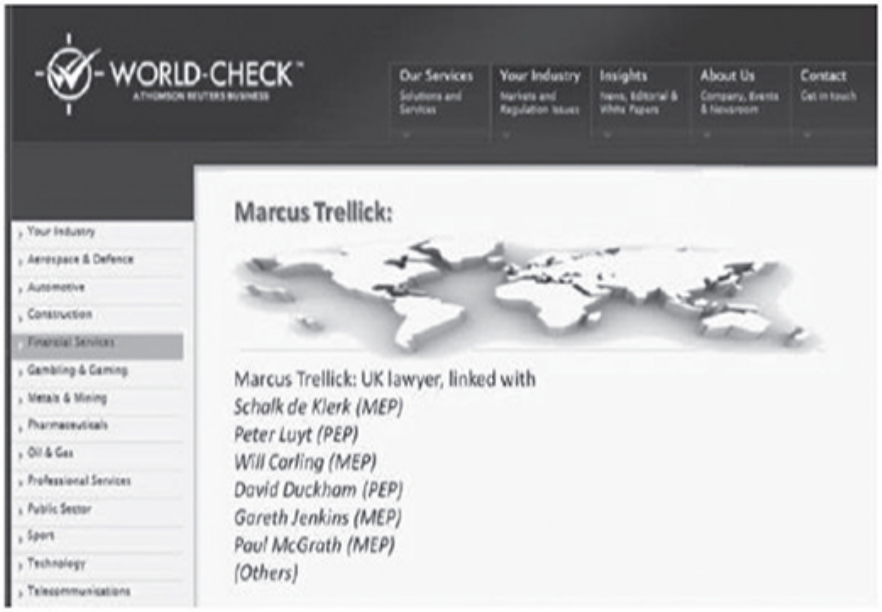
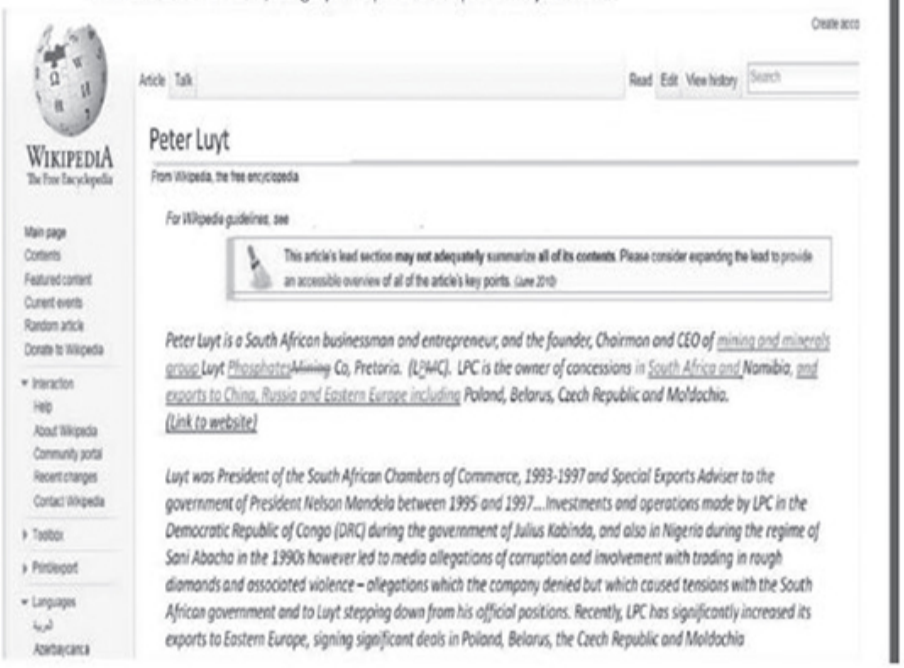


Figure 8.5 **Public and specialist internet searches against Peter Luyt**

Google

In relation to PETER LUYT , Google points you to a Wikipedia entry as follows.



WIKIPEDIA
The Free Encyclopedia

Article Talk

Read Edit View history

Peter Luyt

From Wikipedia, the free encyclopedia

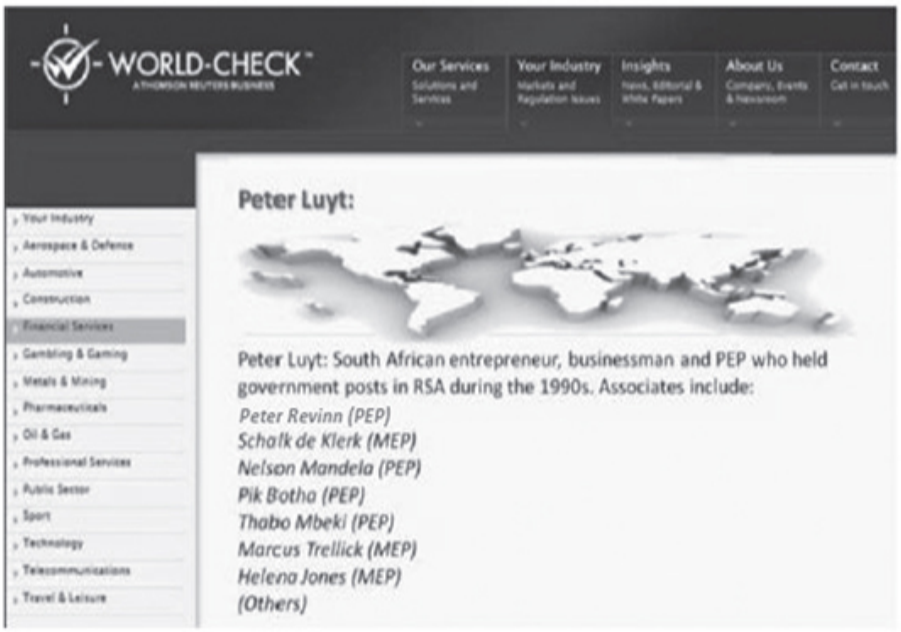
For Wikipedia guidelines, see

This article's lead section may not adequately summarize all of its contents. Please consider expanding the lead to provide an accessible overview of all of the article's key points. (June 2010)

Peter Luyt is a South African businessman and entrepreneur, and the founder, Chairman and CEO of mining and minerals group Luyt Phosphate~~Mining~~ Co, Pretoria. (LPMC). LPC is the owner of concessions in South Africa and Namibia, and exports to China, Russia and Eastern Europe including Poland, Belarus, Czech Republic and Moldochia.
(Link to website)

Luyt was President of the South African Chambers of Commerce, 1993-1997 and Special Exports Adviser to the government of President Nelson Mandela between 1995 and 1997...Investments and operations made by LPC in the Democratic Republic of Congo (DRC) during the government of Julius Kabinda, and also in Nigeria during the regime of Sani Abacha in the 1990s however led to media allegations of corruption and involvement with trading in rough diamonds and associated violence – allegations which the company denied but which caused tensions with the South African government and to Luyt stepping down from his official positions. Recently, LPC has significantly increased its exports to Eastern Europe, signing significant deals in Poland, Belarus, the Czech Republic and Moldochia

A Worldcheck search against Luyt reveals the following pertinent information



WORLD-CHECK
A THOMSON REUTERS BUSINESS

Our Services | Your Industry | Insights | About Us | Contact

Peter Luyt:

Peter Luyt: South African entrepreneur, businessman and PEP who held government posts in RSA during the 1990s. Associates include:

Peter Revinn (PEP)
Schalk de Klerk (MEP)
Nelson Mandela (PEP)
Pik Botha (PEP)
Thabo Mbeki (PEP)
Marcus Trellick (MEP)
Helena Jones (MEP)
(Others)

Figure 8.6 **Public and specialist internet searches against Peter Revinn**

Google

In relation to PETER REVINN, Google points you to a Wikipedia entry as follows.

Peter Revinn is currently Minister of Agriculture in the Government of the Republic of Moldachia (details continue...)

WIKIPEDIA
The Free Encyclopedia

Article Talk | Read Edit View history Search

Peter Revinn

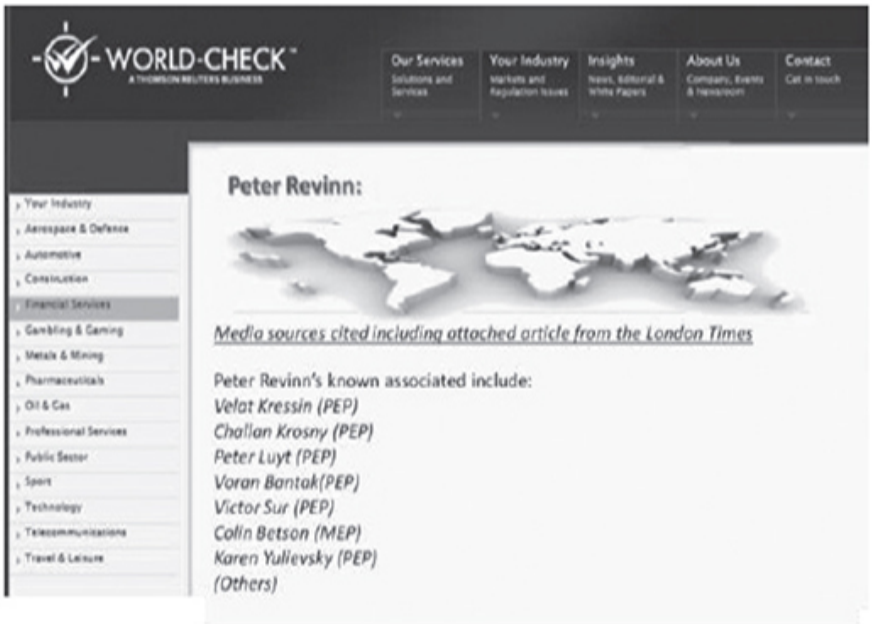
From Wikipedia, the free encyclopedia

For Wikipedia guidelines, see

This article's lead section may not adequately summarize all of its contents. Please consider expanding the lead to provide an accessible overview of all of the article's key points. (June 2010)

Peter Revinn: Minister for Agriculture, Republic of Moldachia, 2010-present. Previously, Minister for Telecommunications 2007-2010. Under-minister in the Transport ministry 2006-2007. Former Vice-Chair, Moldachian National Party (MNP). *Peter Revinn* has been the subject of media allegations of corruption, notably in relation to the award of capital equipment contracts to foreign companies and the privatization of the Moldachian National Telecommunications Company, MoldacTel in 2009. No charges have ever been brought and he has denied the allegations as the work of political opponents sponsored by the opposition Moldachian Democratic Party (MDP).

A Worldcheck search against Peter Revinn reveals the following pertinent information



WORLD-CHECK

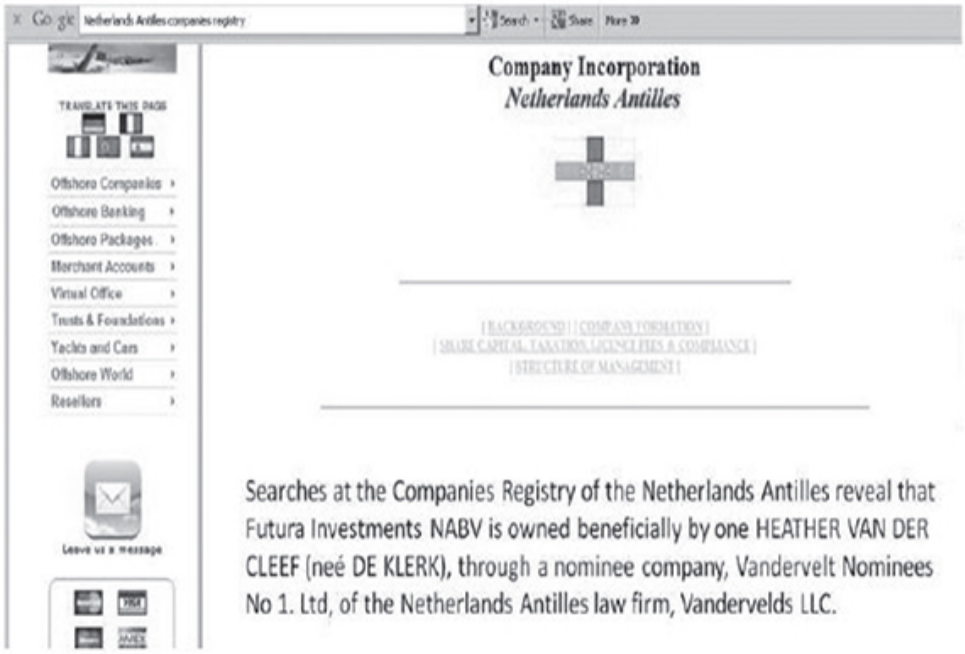
Our Services | Your Industry | Insights | About Us | Contact

Peter Revinn:

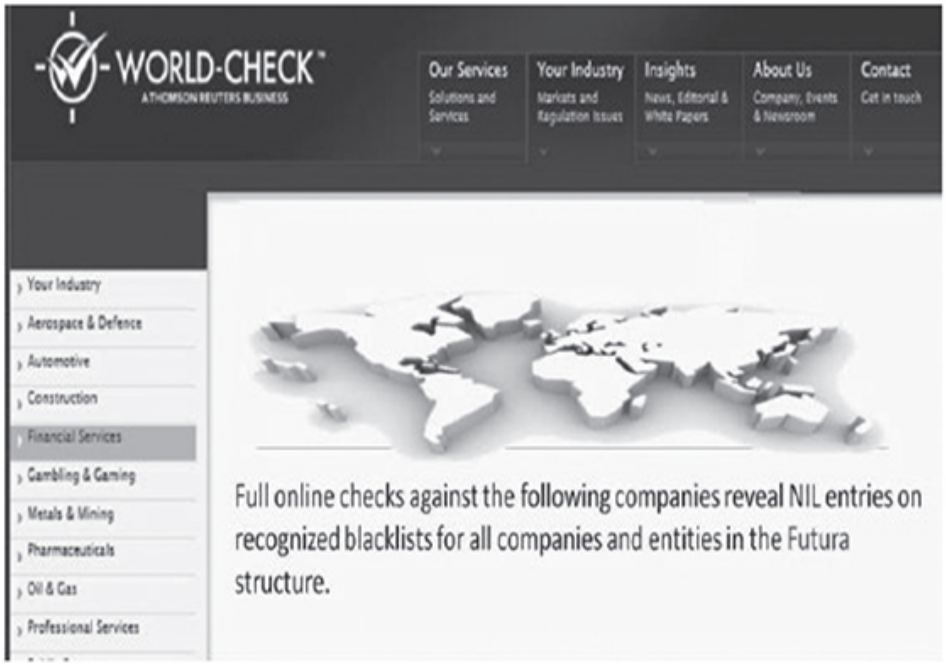
Media sources cited including attached article from the London Times

Peter Revinn's known associated include:
Velat Kressin (PEP)
Challan Krosny (PEP)
Peter Luyt (PEP)
Voran Bantak(PEP)
Victor Sur (PEP)
Colin Betson (MEP)
Karen Yulievsky (PEP)
(Others)

Figure 8.7 **Company searches against Futura Investments NABV**



Searches at the Companies Registry of the Netherlands Antilles reveal that Futura Investments NABV is owned beneficially by one HEATHER VAN DER CLEEF (neé DE KLERK), through a nominee company, Vandervelt Nominees No 1. Ltd, of the Netherlands Antilles law firm, Vandervelds LLC.



Full online checks against the following companies reveal NIL entries on recognized blacklists for all companies and entities in the Futura structure.

DISCUSSION POINTS: FUTURA CAPITAL PARTNERS CASE

Part 1

How would you analyse the risks in this potential relationship?

- On the face of it, this seems like a low-risk relationship. We are dealing with a regulated financial institution within an EU country which is by definition a lower risk for money laundering and terrorist financing.
- The institution itself has AML controls which have presumably passed the stiff tests imposed by its regulator, the AFN, and a large part of the business appears to be from European medium-sized companies, or from high net worth individuals who we can perhaps presume are well known to the two main managers of the company, who each have a solid background in European financial services with well-known corporate names.
- In addition, the directors' details reveal that with one exception, their nationalities, locations and tax domiciles are all of an EU jurisdiction.
- The market reputation of the company appears to be good, and growing. One aspect of the information which stands out as being slightly different from the rest is the identity and role of the two non-executive directors, Roberto di Michele and Schalk de Klerk. You would need to understand who they are,

what their role is within the company, why they are located in Miami and Johannesburg, respectively, and generally to get a clearer picture of their role during due diligence.

■ In addition, the summary refers to 'pension fund placements from a growing number of Dutch and other European medium-sized businesses. . . '. You would want to know more in general terms about the types and geographical locations of the businesses referred to. What sectors do those businesses operate in – financial services, construction, mining and extraction, oil, hotels, land development? Whereabouts in Europe are they located apart from the Netherlands? The Nordic countries? Germany, Italy, France, Britain, Czech Republic, Bulgaria, Romania, Moldachia? If higher-risk locations are involved, you will need to consider Enhanced Due Diligence (EDD) measures on Futura.

What due diligence would be required?

■ Client Due Diligence (CDD) checks against all the directors, including the non-executive directors.

■ If EDD, these checks should encompass the issues such as

– Google, Bing, other search engines

– Factiva, World-check, Templeton Thorp or other screening systems

– international and national press and other media

– in-country staff at your firm, if available

– national registries relating to companies' information, criminal records, bankruptcy

– industry and professional contacts, foreign banks

– conversations with directors themselves (statements made by them can be checked for consistency against independently available information)
– where necessary, special reports commissioned from firms of investigations consultants.

NB: Very important to retain records; that means notes of meetings and phone conversations, printouts of web pages (even negative search results).

■ Note also that EU and international AML standards permit firms to rely on Customer Due Diligence (CDD) undertaken by other financial firms either regulated in the EU or which have AML and CFT regulatory standards which are of the same strength as EU standards. However, the relying firm remains liable for any CDD failures.

■ As a mitigating step, and in order to deal with the problem of obtaining CDD information on, potentially, many thousands of underlying investors, many financial institutions will seek a certificate from a financial intermediary confirming that:

– their AML policies comply with national laws and regulations
– they have identified their own clients
– none of their clients are from prohibited countries
– they have checked source of funds of their investments and that these do not come from criminal activities/are not destined for terrorist activities
– they will keep records and make them available for inspection

– their AML policy covers all their offices, wherever located.

Are there any other issues for consideration?

Yes. In addition, you need to consider your personal position under the Code of Conduct which requires that members of staff should avoid any situation that is liable to give rise to a conflict of interest. In the case of Futura, while your personal relationship with Stanley Hardberg is not stated to be particularly close, nevertheless you do have some kind of personal social relationship going back for a number of years and accordingly it would be inappropriate for you to proceed on this project without discussing the matter first with Compliance.

Part 2

What effect does this information have on your risk assessment of the potential relationship?

Even though the fact of Futura's solid, Dutch, European base and qualified experienced management remains, there are a number of issues here which create some concerns from an AML perspective.

- The involvement of an offshore structure immediately triggers concerns about transparency and tax legality. Firms generally operate policies to control their involvement with OFCs, to prevent themselves becoming involved with money laundering or tax evasion and to keep themselves away from projects involving prohibited jurisdictions. The Netherlands Antilles (which was dissolved as a state in 2010, but which still exists as a place) is not a prohibited jurisdiction under current

international watch-lists, but nevertheless it has an historical association with offshore tax planning and you would therefore need to be clear that the structure is reasonable and acceptable.

- Complex structures and multiple layers of ownership are a red flag requiring further investigation. As disclosed, the structure does not actually reveal the full beneficial ownership of Futura, since we do not know the remaining 75 per cent owners of Futura Investments, which in itself is, indirectly, a significant minority shareholder in Futura itself. EU and international Standards require financial institutions to establish the identity of natural persons owning or controlling 25 per cent or more of the shares or voting rights of any entity with whom they are going to establish business relations (unless they are entitled to apply simplified due diligence as described above), and the same principles would apply here.
- From a governance perspective, note the fact that Mr van der Cleef's father-in-law is a non-executive director of the company. This is not in itself indicative of anything being wrong. Nevertheless, it is characteristic of 'small company behaviour' rather than 'large company behaviour' and this is significant because the whole principle of reliance and introduction certificates is that a firm is able to take a view of robust confidence in the control environment of the potential client. This information weakens that confidence.
- The origin of the funds of the South African clients is also a potential source of concern. Futura may be prepared to sign an introduction certificate to the effect that they are sure that the funds are from legitimate sources, but what degree of

confidence can we have in that? Could foreign exchange restrictions be being breached or could there be tax evasion involved that would create reputational issues?

How should you proceed?

There is essentially a choice here between ‘reliance’ and ‘diligence’. Either you can rely on Futura’s regulated status in an EU country and the apparently sound standing of the directors and the legal opinions issued by a law firm regulated in another EU country – *OR* – you can seek to ‘dig deeper’ into the background of this firm and its underlying relationships. The latter is really what you should do. This could entail:

- Deeper, further enquiries with Futura itself, via Mr Van der Cleef and Mr Hardberg, about Mr de Klerk’s actual role and influence in the company.
- Deeper, further enquiries into the backgrounds and reputations of the two non-executives, Mr de Klerk and Mr de Michele. Mr Luyt, and the nature of Mr de Klerk’s relationship with him.
- Deeper, further enquiries into Marcus Trellick and the law firm Hartwell Mason and their reputation and standing.
- Deeper, further enquiries into the associations of de Klerk and Trellick. This raises an interesting question: namely, how much further do you delve into the relationships and associations of particular individuals and entities? If you do follow-on searches against a common associate, Peter Luyt, you immediately hit ‘trouble’ in the form of the allegations surrounding his involvement with Julius Kabinda and Sani

Abacha, and his dealings with Peter Revinn, the allegedly corrupt Moldachian cabinet minister. Is it possible that, through their relationships with Luyt – and onward into his relations with de Klerk and de Klerk's position inside Futura – that such characters are laundering the proceeds of their corruption through Futura, and hence through your firm?

- Establishing, through research in the public records of the Netherlands Antilles, who the owners of Futura Investments are.
- Deeper, further enquiries into the reputations and standing of other companies within the structure (Futura Financial Management, Futura Nominees and Futura OffshoreHoldings). Do their names appear in any reported cases or newspaper articles?

Part 3

The Real Picture

If you do your due diligence properly in this case and 'follow your nose' from one available information source to the next, you pretty soon find the real picture. Namely, that Futura is being used by Peter Revinn to launder corruption proceeds from Moldachia through the global investment markets, with his involvement being hidden via Peter Luyt, Schalk de Klerk and the law firm Hartwell Mason.

Appendix

The Wolfsberg Group

Financial Institution Name: _____
Location (Country): _____

The questionnaire is required to be answered on a Legal Entity (LE) Level. This means the Financial Institution will answer the questionnaire at an ultimate parent/head office & subsidiary level for which any branches would be considered covered by that parent/subsidiary DDQ. This questionnaire should not cover more than one LE. Each question in the DDQ will need to be addressed from the perspective of the LE and on behalf of all of its branches. If a response for the LE differed for one of its branches this needs to be highlighted and detail regarding this difference captured at the end of each subsection. If a branch business activity (products offered, client base, etc.) is significantly different than its head office, the branch should complete a separate questionnaire.

No #	Question	Answer
1. ENTITY & OWNERSHIP		
1	Full Legal Name	
2	Append a list of branches which are covered by this questionnaire	
3	Full Legal (Registered) Address	
4	Full Primary Business Address (if different from above)	
5	Date of Entity incorporation/establishment	
6	Select type of ownership and append an ownership chart if available	

6 a	Publicly Traded (25% of shares publicly traded)	
6 a1	If Y, indicate the exchange traded on and ticker symbol	
6 b	Member Owned/Mutual	
6 c	Government or State Owned by 25% or more	
6 d	Privately Owned	
6 d1	If Y, provide details of shareholders or ultimate beneficial owners with a holding of 10% or more	
7	% of the Entity's total shares composed of bearer shares	
8	Does the Entity, or any of its branches, operate under an Offshore Banking License (OBL)?	
8 a	If Y, provide the name of the relevant branch/es which operate under an OBL	
9	Name of primary financial regulator/supervisory authority	
10	Provide Legal Entity Identifier (LEI) if available	
11	Provide the full legal name of the ultimate parent (if different from the Entity completing the DDQ)	
12	Jurisdiction of licensing authority and regulator of ultimate parent	
13	Select the business areas applicable to the Entity	
13 a	Retail Banking	
13 b	Private Banking/Wealth Management	
13 c	Commercial Banking	
13 d	Transactional Banking	
13 e	Investment Banking	
13 f	Financial Markets Trading	
13 g	Securities Services/Custody	
13 h	Broker/Dealer	

13 i	Multilateral Development Bank	
13 j	Other	
14	Does the Entity have a significant (10% or more) offshore customer base, either by number of customers or by revenues (where offshore means not domiciled in the jurisdiction where bank services are being provided)?	
14 a	If Y, provide details of the country and %	
15	Select the closest value:	
15 a	Number of employees	
15 b	Total Assets	
16	Confirm that all responses provided in the above Section ENTITY & OWNERSHIP are representative of all the LE's branches	
16 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
16 b	If appropriate, provide any additional information/context to the answers in this section.	
2. PRODUCTS & SERVICES		
17	Does the Entity offer the following products and services:	
17 a	Correspondent Banking	
17 a1	If Y	
17 a2	Does the Entity offer Correspondent Banking services to domestic banks?	
17 a3	Does the Entity allow domestic bank clients to provide downstream relationships?	
17 a4	Does the Entity have processes and procedures in place to identify downstream relationships with domestic banks?	
17 a5	Does the Entity offer correspondent banking services to Foreign Banks?	

17 a6	Does the Entity allow downstream relationships with Foreign Banks?	
17 a7	Does the Entity have processes and procedures in place to identify downstream relationships with Foreign Banks?	
17 a8	Does the Entity offer correspondent banking services to regulated MSBs/MVTS?	
17 a9	Does the Entity allow downstream relationships with MSBs/MVTS?	
17 a10	Does the Entity have processes and procedures in place to identify downstream relationships with MSB/MVTS?	
17 b	Private Banking (domestic & international)	
17 c	Trade Finance	
17 d	Payable Through Accounts	
17 e	Stored Value Instruments	
17 f	Cross Border Bulk Cash Delivery	
17 g	Domestic Bulk Cash Delivery	
17 h	International Cash Letter	
17 i	Remote Deposit Capture	
17 j	Virtual/Digital Currencies	
17 k	Low Price Securities	
17 l	Hold Mail	
17 m	Cross Border Remittances	
17 n	Service to walk-in customers non-account holders)	
17 o	Sponsoring Private ATMs	
17 p	Other high risk products and services identified by the Entity	
18	Confirm that all responses provided in the above Section PRODUCTS & SERVICES are representative of all the LE's branches	

18 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
18 b	If appropriate, provide any additional information/context to the answers in this section.	
3. AML, CTF & SANCTIONS PROGRAMME		
19	Does the Entity have a programme that sets minimum AML, CTF and Sanctions standards regarding the following components:	
19 a	Appointed Officer with sufficient experience/expertise	
19 b	Cash Reporting	
19 c	CDD	
19 d	EDD	
19 e	Beneficial Ownership	
19 f	Independent Testing	
19 g	Periodic Review	
19 h	Policies and Procedures	
19 i	Risk Assessment	
19 j	Sanctions	
19 k	PEP Screening	
19 l	Adverse Information Screening	
19 m	Suspicious Activity Reporting	
19 n	Training and Education	
19 o	Transaction Monitoring	
20	How many full time employees are in the Entity's AML, CTF & Sanctions Compliance Department?	
21	Is the Entity's AML, CTF & Sanctions policy approved at least annually by the Board or equivalent Senior Management Committee?	

22	Does the Board or equivalent Senior Management Committee receive regular reporting on the status of the AML, CTF & Sanctions programme?	
23	Does the Entity use third parties to carry out any components of its AML, CTF & Sanctions programme?	
23 a	If Y, provide further details	
24	Confirm that all responses provided in the above Section AML, CTF & SANCTIONS Programme are Representative of all the LE's branches	
24 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
24 b	If appropriate, provide any additional information/context to the answers in this section.	
4. ANTI BRIBERY & CORRUPTION		
25	Has the Entity documented policies and procedures consistent with applicable ABC regulations and requirements to [reasonably] prevent, detect and report bribery and corruption?	
26	Does the Entity have an enterprise wide programme that sets minimum ABC standards?	
27	Has the Entity appointed a designated officer or officers with sufficient experience/expertise responsible for coordinating the ABC programme?	
28	Does the Entity have adequate staff with appropriate levels of experience/expertise to implement the ABC programme?	
29	Is the Entity's ABC programme applicable to:	
29 a	Joint ventures	
29 b	Third parties acting on behalf of the Entity	
30	Does the Entity have a global ABC policy that:	

30 a	Prohibits the giving and receiving of bribes? This includes promising, offering, giving, solicitation or receiving of anything of value, directly or indirectly, if improperly intended to influence action or obtain an advantage	
30 b	Includes enhanced requirements regarding interaction with public officials?	
30 c	Includes a prohibition against the falsification of books and records (this may be within the ABC policy or any other policy applicable to the Legal Entity)?	
31	Does the Entity have controls in place to monitor the effectiveness of their ABC programme?	
32	Does the Entity's Board or Senior Management Committee receive regular Management Information on ABC matters?	
33	Does the Entity perform an Enterprise Wide ABC risk assessment?	
33 a	If Y select the frequency	
34	Does the Entity have an ABC residual risk rating that is the net result of the controls effectiveness and the inherent risk assessment?	
35	Does the Entity's ABC EWRA cover the inherent risk components detailed below:	
35 a	Potential liability created by intermediaries and other third-party providers as appropriate	
35 b	Corruption risks associated with the countries and industries in which the Entity does business, directly or through intermediaries	
35 c	Transactions, products or services, including those that involve state-owned or state-controlled entities or public officials	
35 d	Corruption risks associated with gifts and hospitality, hiring/internships, charitable donations and political contributions	
35 e	Changes in business activities that may materially increase the Entity's corruption risk	

36	Does the Entity's internal audit function or other independent third party cover ABC Policies and Procedures?	
37	Does the Entity provide mandatory ABC training to:	
37 a	Board and Senior Committee Management	
37 b	1st Line of Defence	
37 c	2nd Line of Defence	
37 d	3rd Line of Defence	
37 e	3rd parties to which specific compliance activities subject to ABC risk have been outsourced	
37 f	Non-employed workers as appropriate (contractors/consultants)	
38	Does the Entity provide ABC training that is targeted to specific roles, responsibilities and activities?	
39	Confirm that all responses provided in the above Section Anti Bribery & Corruption are representative of all the LE's branches	
39 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
39 b	If appropriate, provide any additional information/context to the answers in this section.	
5. POLICIES & PROCEDURES		
40	Has the Entity documented policies and procedures consistent with applicable AML, CTF & Sanctions regulations and requirements to reasonably prevent, detect and report:	
40 a	Money laundering	
40 b	Terrorist financing	
40 c	Sanctions violations	
41	Are the Entity's policies and procedures updated at least annually?	

42	Are the Entity's policies and procedures gapped against/compared to:	
42 a	US Standards	
42 a1	If Y, does the Entity retain a record of the results?	
42 b	EU Standards	
42 b1	If Y, does the Entity retain a record of the results?	
43	Does the Entity have policies and procedures that:	
43 a	Prohibit the opening and keeping of anonymous and fictitious named accounts	
43 b	Prohibit the opening and keeping of accounts for unlicensed banks and/or NBFIs	
43 c	Prohibit dealing with other entities that provide banking services to unlicensed banks	
43 d	Prohibit accounts/relationships with shell banks	
43 e	Prohibit dealing with another entity that provides services to shell banks	
43 f	Prohibit opening and keeping of accounts for Section 311 designated entities	
43 g	Prohibit opening and keeping of accounts for any of unlicensed/unregulated remittance agents, exchanges houses, casa de cambio, bureaux de change or money transfer agents	
43 h	Assess the risks of relationships with PEPs, including their family and close associates	
43 i	Define escalation processes for financial crime risk issues	
43 j	Define the process, where appropriate, for terminating existing customer relationships due to financial crime risk	
43 k	Specify how potentially suspicious activity identified by employees is to be escalated and investigated	
43 l	Outline the processes regarding screening for sanctions, PEPs and negative media	

43 m	Outline the processes for the maintenance of internal “watchlists”	
44	Has the Entity defined a risk tolerance statement or similar document which defines a risk boundary around their business?	
45	Does the Entity have a record retention procedures that comply with applicable laws?	
45 a	If Y, what is the retention period?	
46	Confirm that all responses provided in the above Section POLICIES & PROCEDURES are representative of all the LE’s branches	
46 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
46 b	If appropriate, provide any additional information/context to the answers in this section.	
6. AML, CTF & SANCTIONS RISK ASSESSMENT		
47	Does the Entity’s AML & CTF EWRA cover the inherent risk components detailed below:	
47 a	Client	
47 b	Product	
47 c	Channel	
47 d	Geography	
48	Does the Entity’s AML & CTF EWRA cover the controls effectiveness components detailed below:	
48 a	Transaction Monitoring	
48 b	Customer Due Diligence	
48 c	PEP Identification	
48 d	Transaction Screening	
48 e	Name Screening against Adverse Media & Negative News	
48 f	Training and Education	

48 g	Governance	
48 h	Management Information	
49	Has the Entity's AML & CTF EWRA been completed in the last 12 months?	
49 a	If N, provide the date when the last AML & CTF EWRA was completed.	
50	Does the Entity's Sanctions EWRA cover the inherent risk components detailed below:	
50 a	Client	
50 b	Product	
50 c	Channel	
50 d	Geography	
51	Does the Entity's Sanctions EWRA cover the controls effectiveness components detailed below:	
51 a	Customer Due Diligence	
51 b	Transaction Screening	
51 c	Name Screening	
51 d	List Management	
51 e	Training and Education	
51 f	Governance	
51 g	Management Information	
52	Has the Entity's Sanctions EWRA been completed in the last 12 months?	
52 a	If N, provide the date when the last Sanctions EWRA was completed.	
53	Confirm that all responses provided in the above Section AML, CTF & SANCTIONS RISK ASSESSMENT are representative of all the LE's branches	
53 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	

53 b	If appropriate, provide any additional information/context to the answers in this section.	
7. KYC, CDD and EDD		
54	Does the Entity verify the identity of the customer?	
55	Do the Entity's policies and procedures set out when CDD must be completed, e.g. at the time of onboarding or within 30 days	
56	Which of the following does the Entity gather and retain when conducting CDD? Select all that apply:	
56 a	Ownership structure	
56 b	Customer identification	
56 c	Expected activity	
56 d	Nature of business/employment	
56 e	Product usage	
56 f	Purpose and nature of relationship	
56 g	Source of funds	
56 h	Source of wealth	
57	Are each of the following identified:	
57 a	Ultimate beneficial ownership	
57 a1	Are ultimate beneficial owners verified?	
57 b	Authorised signatories (where applicable)	
57 c	Key controllers	
57 d	Other relevant parties	
58	What is the Entity's minimum (lowest) threshold applied to beneficial ownership identification?	
59	Does the due diligence process result in customers receiving a risk classification?	
60	If Y, what factors/criteria are used to determine the customer's risk classification? Select all that apply:	

60 a	Product Usage	
60 b	Geography	
60 c	Business Type/Industry	
60 d	Legal Entity type	
60 e	Adverse Information	
60 f	Other (specify)	
61	Does the Entity have a risk based approach to screening customers for adverse media/negative news?	
62	If Y, is this at:	
62 a	Onboarding	
62 b	KYC renewal	
62 c	Trigger event	
63	What is the method used by the Entity to screen for adverse media/negative news?	
63 a	Automated	
63 b	Manual	
63 c	Combination of automated and manual	
64	Does the Entity have a risk based approach to screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
65	If Y, is this at:	
65 a	Onboarding	
65 b	KYC renewal	
65 c	Trigger event	
66	What is the method used by the Entity to screen PEPs?	
66 a	Automated	

66 b	Manual	
66 c	Combination of automated and manual	
67	Does the Entity have policies, procedures and processes to review and escalate potential matches from screening customers and connected parties to determine whether they are PEPs, or controlled by PEPs?	
68	Does the Entity have a process to review and update customer information based on:	
68 a	KYC renewal	
68 b	Trigger event	
69	Does the Entity maintain and report metrics on current and past periodic or trigger event due diligence reviews?	
70	From the list below, which categories of customers or industries are subject to EDD and/or are restricted, or prohibited by the Entity's FCC programme?	
70 a	Non-account customers	
70 b	Offshore customers	
70 c	Shell banks	
70 d	MVTS/MSB customers	
70 e	PEPs	
70 f	PEP Related	
70 g	PEP Close Associate	
70 h	Correspondent Banks	
70 h1	If EDD or EDD & Restricted, does the EDD assessment contain the elements as set out in the Wolfsberg Correspondent Banking Principles 2014?	
70 i	Arms, defense, military	
70 j	Atomic power	
70 k	Extractive industries	

70 l	Precious metals and stones	
70 m	Unregulated charities	
70 n	Regulated charities	
70 o	Red light business/Adult entertainment	
70 p	Non-Government Organisations	
70 q	Virtual currencies	
70 r	Marijuana	
70 s	Embassies/Consulates	
70 t	Gambling	
70 u	Payment Service Provider	
70 v	Other (specify)	
71	If restricted, provide details of the restriction	
72	Does the Entity perform an additional control or quality review on clients subject to EDD?	
73	Confirm that all responses provided in the above Section KYC, CDD and EDD are representative of all the LE's branches	
73 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to	
73 b	If appropriate, provide any additional information/context to the answers in this section.	
8. MONITORING & REPORTING		
74	Does the Entity have risk based policies, procedures and monitoring processes for the identification and reporting of suspicious activity?	
75	What is the method used by the Entity to monitor transactions for suspicious activities?	
75 a	Automated	
75 b	Manual	
75 c	Combination of automated and manual	

76	If manual or combination selected, specify what type of transactions are monitored manually	
77	Does the Entity have regulatory requirements to report currency transactions?	
77 a	If Y, does the Entity have policies, procedures and - processes to comply with currency reporting requirements?	
78	Does the Entity have policies, procedures and processes to review and escalate matters arising from the monitoring of customer transactions and activity?	
79	Confirm that all responses provided in the above Section MONITORING & REPORTING are representative of all the LE's branches	
79 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to	
79 b	If appropriate, provide any additional information/context to the answers in this section.	
9. PAYMENT TRANSPARENCY		
80	Does the Entity adhere to the Wolfsberg Group Payment Transparency Standards?	
81	Does the Entity have policies, procedures and processes to [reasonably] comply with and have controls in place to ensure compliance with:	
81 a	FATF Recommendation 16	
81 b	Local Regulations	
81 b1	Specify the regulation	
81 c	If N, explain	
82	Does the Entity have processes in place to respond to Request For Information (RFIs) from other entities in a timely manner?	
83	Does the Entity have controls to support the inclusion of required and accurate originator information in international payment messages?	

84	Does the Entity have controls to support the inclusion of required beneficiary in international payment messages?	
85	Confirm that all responses provided in the above Section PAYMENT TRANSPARENCY are representative of all the LE's branches	
85 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
85 b	If appropriate, provide any additional information/context to the answers in this section.	
10. SANCTIONS		
86	Does the Entity have a Sanctions Policy approved by management regarding compliance with sanctions law applicable to the Entity, including with respect its business conducted with, or through accounts held at foreign financial institutions?	
87	Does the Entity have policies, procedures, or other controls reasonably designed to prevent the use of another entity's accounts or services in a manner causing the other entity to violate sanctions prohibitions applicable to the other entity (including prohibitions within the other entity's local jurisdiction)?	
88	Does the Entity have policies, procedures or other controls reasonably designed to prohibit and/or detect actions taken to evade applicable sanctions prohibitions, such as stripping, or the resubmission and/or masking, of sanctions relevant information in cross border transactions?	
89	Does the Entity screen its customers, including beneficial ownership information collected by the Entity, during onboarding and regularly thereafter against Sanctions Lists?	
90	What is the method used by the Entity?	
90 a	Manual	
90 b	Automated	
90 c	Combination of Automated and Manual	

91	Does the Entity screen all sanctions relevant data, including at a minimum, entity and location - information, contained in cross border transactions against Sanctions Lists?	
92	What is the method used by the Entity?	
92 a	Manual	
92 b	Automated	
92 c	Combination Automated and Manual	
93	Select the Sanctions Lists used by the Entity in its sanctions screening processes:	
93 a	Consolidated United Nations Security Council Sanctions List (UN)	
93 b	United States Department of the Treasury's Office of Foreign Assets Control (OFAC)	
93 c	Office of Financial Sanctions Implementation HMT (OFSI)	
93 d	European Union Consolidated List (EU)	
93 e	Lists maintained by other G7 member countries	
93 f	Other (specify)	
94	When new entities and natural persons are added to sanctions lists, how many business days before the Entity updates its lists?	
95	When updates or additions to the Sanctions Lists are made, how many business days before the Entity updates their active manual and/or automated screening system against:	
95 a	Customer Data	
95 b	Transactions	
96	Does the Entity have a physical presence, e.g., branches, subsidiaries, or representative offices located in countries/regions against which UN, OFAC, OFSI, EU and G7 member countries have enacted comprehensive jurisdiction-based Sanctions?	

97	Confirm that all responses provided in the above Section SANCTIONS are representative of all the LE's branches	
97 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
97 b	If appropriate, provide any additional information/context to the answers in this section.	
11. TRAINING & EDUCATION		
98	Does the Entity provide mandatory training, which includes:	
98 a	Identification and reporting of transactions to government authorities	
98 b	Examples of different forms of money laundering, terrorist financing and sanctions violations relevant for the types of products and services offered	
98 c	Internal policies for controlling money laundering, terrorist financing and sanctions violations	
98 d	New issues that occur in the market, e.g., significant regulatory actions or new regulations	
98 e	Conduct and Culture	
99	Is the above mandatory training provided to:	
99 a	Board and Senior Committee Management	
99 b	1st Line of Defence	
99 c	2nd Line of Defence	
99 d	3rd Line of Defence	
99 e	3rd parties to which specific FCC activities have been outsourced	
99 f	Non-employed workers (contractors/consultants)	
100	Does the Entity provide AML, CTF & Sanctions training that is targeted to specific roles, responsibilities and high risk products, services and activities?	

101	Does the Entity provide customised training for AML, CTF and Sanctions staff?	
102	Confirm that all responses provided in the above Section TRAINING & EDUCATION are representative of all the LE's branches	
102 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
102 b	If appropriate, provide any additional information/context to the answers in this section.	
12. QUALITY ASSURANCE/COMPLIANCE TESTING		
103	Are the Entity's KYC processes and documents subject to quality assurance testing?	
104	Does the Entity have a program wide risk based Compliance Testing process (separate to the independent Audit function)?	
105	Confirm that all responses provided in the above Section QUALITY ASSURANCE/COMPLIANCE TESTING are representative of all the LE's branches	
105 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
105 b	If appropriate, provide any additional information/context to the answers in this section.	
13. AUDIT		
106	In addition to inspections by the government supervisors/regulators, does the Entity have an internal audit function, a testing function or other independent third party, or both, that assesses FCC AML, CTF and Sanctions policies and practices on a regular basis?	
107	How often is the Entity audited on its AML, CTF & Sanctions programme by the following:	
107 a	Internal Audit Department	
107 b	External Third Party	

108	Does the internal audit function or other independent third party cover the following areas:	
108 a	AML, CTF & Sanctions policy and procedures	
108 b	KYC/CDD/EDD and underlying methodologies	
108 c	Transaction Monitoring	
108 d	Transaction Screening including for sanctions	
108 e	Name Screening & List Management	
108 f	Training & Education	
108 g	Technology	
108 h	Governance	
108 i	Reporting/Metrics & Management Information	
108 j	Suspicious Activity Filing	
108 k	Enterprise Wide Risk Assessment	
108 l	Other (specify)	
109	Are adverse findings from internal & external audit tracked to completion and assessed for adequacy and completeness?	
110	Confirm that all responses provided in the above Section, AUDIT are representative of all the LE's branches	
110 a	If N, clarify which questions the difference/s relate to and the branch/es that this applies to.	
110 b	If appropriate, provide any additional information/context to the answers in this section.	

DECLARATION STATEMENT

Wolfsberg Group Correspondent Banking Due Diligence Questionnaire 2018 (CBDDQ V1.2)

Declaration Statement (To be signed by Global Head of Correspondent Banking or equivalent position holder AND Group Money Laundering Prevention Officer, Global Head of Anti- Money Laundering, Chief Compliance Officer, Global Head of Financial Crimes Compliance OR equivalent)

_____ (Bank name) is fully committed to the fight against financial crime and makes every effort to remain in full compliance with all applicable financial crime laws, regulations and standards in all of the jurisdictions in which it does business and holds accounts.

_____ (Bank name) understands the critical importance of having effective and Sustainable controls to combat financial crime in order to protect its reputation and to meet its legal and regulatory obligations.

_____ (Bank name) recognises the importance of transparency regarding parties to transactions in international payments and has adopted/is committed to adopting these standards.

_____ (Bank name) further certifies it complies with/is working to comply with the Wolfsberg Correspondent Banking Principles and the Wolfsberg Trade Finance Principles. The information provided in this Wolfsberg CBDDQ will be kept current and will be updated no less frequently than on an annual basis.

_____ (Bank name) commits to file accurate supplemental information on a timely basis.

I, _____ (Global Head of Correspondent Banking or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of _____

I, _____ (MLRO or equivalent), certify that I have read and understood this declaration, that the answers provided in this Wolfsberg CBDDQ are complete and correct to my honest belief, and that I am authorised to execute this declaration on behalf of _____ (Bank name)

_____ (Signature & Date)

_____ (Signature & Date)

Cover
Title
Copyright
Contents
Acknowledgement
Disclaimer
Introduction
About the author

1 Fundamental Concepts

Background and definitions
Key processes in money laundering and terrorist financing
Money laundering
Crypto-Laundering and the Blockchain
Terrorist financing
Further differences between terrorist financing and classical money laundering
Suspicion recognition

2 The International AML and CFT Framework

Key components of the international institutional and legal framework
A developing framework to combat tax evasion
Proliferation Financing
A developing framework for the regulation of cryptocurrencies
The Financial Action Task Force (FATF)
FATF regional style bodies and associate members

Other relevant international bodies

Key requirements for financial institutions

Key components of a national AML/CFT framework

3 The Role, Structure and Positioning of the AML/CFT Compliance Function

Structure and culture

AML/CFT best practice

Best practice in higher-risk products and services

IT systems

The use of artificial intelligence

Training, communication and awareness

A ‘pro-business’ approach

Management of internal suspicion reporting

4 CDD, KYC and the Risk-based Approach

Background to the Risk-Based Approach

Components of the Risk-Based Approach

Mitigating controls

Regulatory environment

Special categories: Politically Exposed Persons (PEPs)

Constructing a Risk-Based Approach for your organisation

The core components of CDD

CDD processes and tools

Example risk assessment frameworks

Constructing a CDD framework for financial institutions

Constructing a CDD framework for retail/consumer banking business

Constructing a CDD framework for private banking

5 Reputational Risk

Managing reputational risk

When banks go wrong: cases of punishments and penalties

Managing reputational risk: the experience of the MDBs

The integrity ‘red flags’ checklist and the due diligence investigation tools

Practical application

6 Suspicion Recognition

Background and general principles

Money laundering typologies

Terrorist financing typologies

Account analysis examples

‘Accumulation of evidence’ cases

The 21st century: areas of rising concern

7 International Cooperation

Background

Modern structures of organised crime and terrorism

Mechanisms and tools of international cooperation

International cooperative bodies

8 Modern Money Laundering and Terrorist Financing: Two Case Studies

Introduction

Smoke and Mirrors: AlnaBank and the Messengers of God

Futura Capital Partners: Modern Money Laundering through ‘low risk’ regulated OECD Financial Institutions
Discussion Points: Futura Capital Partners Case
Appendix
Index
toc

Index

ABN AMRO 195
account analysis examples 233, 264–79
account monitoring *see* transaction surveillance/monitoring
'accumulation of evidence' cases 233, 280–4
Akahoshi, Laura 193
al-Baghdadi, Abu Bakr 20
algorithmic trading 35, 36
Al-Qaeda 18, 20, 28, 187, 301
Al Rajhi Bank 187
alternative remittance services (ARS) 233–5
Althorp Investment Co Limited 205
AML/CFT unit 64–5
Animal Liberation Front 305
anonymous bank accounts 32, 45–6, 169, 179
Anti-Money Laundering Group (AMG) 70–1, 74, 77–8
arms trade 157
Artificial Intelligence (AI) xi, xiv, 103–5, 288
    application in customer due diligence 104
    application in transaction surveillance 104–5
    defined 103
Aryan Front 305
Asch, Solomon 67
Ashburton Limited 205

Asia/Pacific Group on Money Laundering (APG) 53
assets
    confiscation of 47, 53
    freezing of 28, 33, 47, 53
assurance activities 64, 79, 125
asymmetrical threat 304
ATMs 19, 90
auctions 236–8
auditbot 105
audit department 64, 72
audit function 63, 75, 79, 86, 125
Australia xi, 37
    cryptocurrency regulation 44, 45
Australia Banking Corporation 190–1
Australian Transaction Report and Analysis Centre (AUSTRAC) 190
Austria 45–6
awareness, culture of 74, 76, 86, 105, 125–6

Bank for International Settlements (BIS) 122
banks
    criminally owned or sympathetic 8
    pocket 245, 320
    shell 8, 36, 50, 57, 90, 168, 179, 195, 245, 246
    unlicensed 168, 179
Bank Secrecy Act, US 37, 204
Basel AML Index 96
Basel Committee on Banking Supervision (BCBS) 54–5, 79–80
bearer share issuers 159, 169, 175, 179, 188
beneficial ownership 30, 31, 32, 37, 49, 52, 55, 57, 80, 208–9, 316, 318–19
beneficiary information 82, 92, 246, 262

best practice 56
customer identification and due diligence 80–3
in higher-risk products and services 89–98
business through intermediaries 95–6
charities and NPOs 96–8
correspondent banking accounts 89–90
best practice (continued)
customers from high-risk geographic locations 96
electronic banking 90–1
politically exposed persons 94, 95
private banking 92–4
unusual/purposeless transaction 95
wire transfers 91–2
internal controls and independent audit 86
name screening 86–9
record-keeping requirements 83–4
reporting obligations 84–6
staff training and awareness 86
Birkenstock, Bradley 193
Bitcoin xi, 8, 12, 14, 15, 15–16, 17, 45
blacklists 28, 65, 75, 210
black market peso exchange 238–40
Blockchain xi, xiv, 12–14, 17
‘blood’ diamonds 240–2
Borgen, Thomas 189
bribery 60, 189, 215
Browder, Bill 10
Bruun & Hjeijle 188, 189
Budovsky, Arthur 17
business accounts 258–9
business ownership approach 70–7
business purpose 56

business sector risk assessment 144, 146, 147
business type 123, 126

Canada 37
Caribbean Financial Action Task Force (CFATF) 53
cash 7, 19
cash couriers 52
cash intensive businesses 7
cash transactions 31, 85–6
casinos 157, 175, 242–4
Castaˇnon, Paulina 198
Cecere, Andy 191
Central Intelligence Agency (CIA) 128
centralised ledger model 13
certification, staff training 108
charities 5, 18, 19, 96–9, 144, 256–7, 263
China 43
    cryptocurrency regulation 44–5
Citibank 2–3, 196–204
Cititrust 197–8
client *see* customer
Coinhive 290
Colombia 37
Common Reporting Standard 41
communication of requirements 72–8
complex ownership structures 37, 81, 159, 175, 209, 319
Compliance Champions 71–2, 75, 77
compliance culture xiii, 65–79
Compliance Officers 65, 68, 69, 70, 72, 75
    pro-business approach 114–15
Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA) (2010), US 42–3, 87

concentration accounts 179, 198
confidentiality 39
  breach of 48, 51, 85, 302
confiscation of assets 47, 53
consolidation 6
contract, breach of 32
cooperation 58
  see also international cooperation
corporate clients
  with complex ownership structures 37, 81, 159, 175, 209, 319
  customer due diligence (CDD)
    documentation requirements 150–3
    example cases 160–5
    framework construction 153–6
    non-personal information 139–40
    personal information 139
    risk calculator tool 157, 158
    risk classification 157–65
corporate governance 207, 215–16
corporate treasury foreign exchange services 131–2
correspondent banking 30, 36, 50, 55, 89–90, 167–8, 169, 244–6, 316, 317
Correspondent Banking Due Diligence Questionnaire (CBDDQ) 90, 170
corruption 10, 215, 284, 294–7, 301, 314–15
Corruption Perceptions Index (CPI) 96, 128
Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) 53, 309
Counter-Terrorism Committee (CTC) 28
country of origin 80
country risk 96, 123, 126, 143–4, 145, 175

see also geographic risk
credit cards 19, 131, 247–9
criminal causation, circle of 302
Criminal Finances Act (2017), UK 37, 38, 41–2
criminalisation 47, 48
criminality 209–10, 215
crowd funding 293
cryptocurrencies (virtual currencies) xi, xiii, 8, 12–18, 32, 44–5, 50, 284, 289–92
cultural organisations 5
currency exchange offices, licensing/registration system 30
currency transaction reporting 85–6
customer acceptance 65, 78–9, 80–1, 93, 113
management approvals required for 81, 124
process flow 100, 102
customer due diligence (CDD) xi, 79, 113, 125, 313–14, 315–17, 321–3, 334
application of AI in 104
best practice 80–3
core components of 138–41
for corporate/wholesale banking business 153–6, 159–65
documentation tools 150–3
EU Money Laundering Directives 30, 31
FATF recommendations 49–50, 51
for financial institutions 56–7, 166–73
higher-risk products and services 93, 95
for private banking 93, 178–83
processes and tools 141–53
for retail/consumer banking business 174–8
US Final Rule on xi, 37
see also enhanced due diligence; integrity due diligence; normal due diligence; simplified due diligence

customer identification 56, 75, 80, 81–2, 91, 93, 113, 124
    corporates 151, 152
customer screening 78–9
customer type 122, 126

Danske Bank 188–9
dark trading 35
dark web xi
data protection 39, 47
de-centralised ledger model 12–14
Deferred Prosecution Agreement (DPA) protocol xiv
Designated Non-Financial Businesses and Professions (DNFBPs) 47, 51–2, 53
detection scenarios 99, 125
Deutsche Bank 189–90
diamond trading 157, 240–2
diaspora-owned businesses 258–9
distribution channels 123–4, 126
Donat Investments SA 197
'donor' businesses 18
drugs trade 15, 19, 26, 238–9, 321
due diligence 40
    research tools 208, 214
    see also customer due diligence
dynamic risk assessment xi

Earth Liberation Front 305
Eastern Europe 46, 85
Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) 53
Egmont Group 55, 309
e-learning 107, 108, 109
electronic banking 90–1

Elliott, Amy 2–4, 196, 197, 198, 199, 203
enhanced due diligence (EDD) 137, 319, 334
corporate clients 153, 157, 159, 160–2, 163–4
correspondent banking 30, 36
and country risk 32, 175
financial institutions 56–7, 168, 169, 171, 172–3
higher-risk accounts 93–4
politically exposed persons (PEP) 30, 31, 157, 174, 211–12
private banking 36, 182
retail/consumer banking business 174–6, 177, 178
and source of wealth information 146
Ethereum 12, 17
Eurasina Group (EAG) 53
European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime (1990) 29
European Convention on the Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, and on the Financing of Terrorism (2005) 29
European Union (EU) 41
Action Plan against terrorism 32
Council Common Position (2001/932/CFSP) 32–5
country risk assessment 144
Iran sanctions 43
Markets in Financial Instruments Directive (Mifid I and II) 35–6
Money Laundering Directives 29–32, 44, 122
e-wallets 293
extradition 53, 307

Failing to Prevent offences xi
false positives xiii, 89, 104, 113
Federal Bureau of Investigation (FBI) 210
Federal Reserve, US 186
fiat currencies xi, 8, 17–18

fie-chien system 234
Figueiredo, Reynaldo 197
Financial Action Task Force (FATF) 42, 45–53, 79, 80, 84, 143, 231–2, 284–5, 301, 308
  40 Recommendations 29–30, 46–53, 58, 83, 85, 91–2, 112, 120, 122, 127, 316
  'Financing of Recruitment for Terrorist Purposes' report (2018) 293
  International Cooperation Review Group (ICRG) 58, 80, 309
  regional style bodies and associate members 53–4
Financial Assets Act (VFA), Malta 44
Financial Conduct Authority, UK 186, 190
Financial Crime Compliance Questionnaire (FCCQ) 90, 170
Financial Crimes Enforcement Network (FinCEN), US 192, 195, 285
financial institutions 47, 52, 53
  customer due diligence (CDD) 56–7, 166–73
  foreign (FFIs) 40
  international (IFIs) 207–14
  key requirements for 56–8
financial instruments, trading in 35–6
Financial Intelligence Units (FIUs) 32, 51, 52, 54, 55, 59
Financial Sector Assessment Programme (FSAP) 54
FinCEN 192, 195, 285
Foreign Account Tax Compliance Act (FATCA) (2010), US xi, 40–1
foreign financial institutions (FFIs) 40
forged identities 82
France 37, 43
fraud 9, 113, 284, 294–7
freezing of assets 28, 33, 47
fronts 7, 18, 19, 256–7, 318, 320
fund management 132

funds transfers
originator and beneficiary information 81, 82, 92, 246, 262
overseas 7, 8, 261–2
see also wire transfers
fungibility 17
Futura Group case study 323–36

GAFI (Groupe d'Action Financière) *see* Financial Action Task Force (FATF)
GAFISUD (Grupo de Accion Financiera Sud America) 53
gambling concerns 157, 175
geographic risk 96, 120, 122, 123, 126, 133, 135, 175
see also country risk
Germany 43
Gibraltar
cryptocurrency regulation xi, 44
Digital Technology Ledger Framework 44
Gibraltar Financial Services Commission (GFSC) 44
government-owned and controlled bodies 159
GRAPO 33
Grupo de Accion Financiera Sud America (GAFISUD) 53

HAMAS 33
hawala system 19, 234
hedge funds 132
Hermitage Asset Management 10, 294
higher-risk customers 83
see also politically exposed persons (PEP)
higher-risk products and services, best practice in *see under* best practice
high-frequency algorithmic trading 35
Hitchcock Investments SA 197
Hokuriku Bank 187

household insurance 133
HSBC 187–8
humanitarian organisations 256–7, 263
human smuggling/trafficking 284–9
hundi system 19, 234

identification *see* customer identification
identity theft 113
import–export businesses 144, 255, 259
information collection 138–40, 159
information sharing 38, 47, 51
information verification *see* verification
ING Bank 193–5
initial coin offerings (ICOs) 45
insurance policies 7, 249–52
    household 133
integration of laundered assets 5, 12, 236
integrity, institutional/individual 60, 186–7, 207
integrity due diligence (IDD) 207–28
    initial stage 208–10
    practical application 216–28
    red flags checklist 208, 214–16
    secondary stage 211–14
interdiction, theory of 302
Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) 53
intermediaries 55, 95–6
International Association of Insurance Supervisors (IAIS) 55, 80
international business transactions 258–9
international cooperation 53, 299–302
    agency level 300
    bodies 58, 80, 308–9

see also Financial Action Task Force
challenges to 301–2
institutional/individual level 300
mechanisms and tools of 306–8
state/governmental level 300
International Cooperation Review Group (ICRG) 58, 80, 309
International Financial Institutions (IFIs) 207–14
International Labour Organization (ILO) 285
international legal framework 26–36
International Monetary Fund (IMF) 45, 54, 79, 81, 90, 95, 95–6
international organised crime 300, 302–5, 314–15
International Organization of Securities Commissions (IOSCO) 55, 80
internet banking 90–1
Interpol 309
investigating authorities 52, 60
see also Federal Bureau of Investigation (FBI); police forces
investment firms, criminally owned or sympathetic 8
investment policies 7
invoicing 7, 254–5, 320
IRA 18, 19–20, 33
Iran 195
sanctions against 42, 43, 87
WMD development 42–4
Iran Nuclear Deal 43
Iran Transactions Regulations (1996), US 43
Ireland xi, 37
ISIS xi, 18, 20
IT systems 98–102
combined systems 100, 102
name check portals/filter systems 98–9
transaction surveillance 99–100

Japan 44, 45, 54
Jemaal Islamiyah 18
Jenkins, Brian 305
Joint Comprehensive Plan of Action (JCPOA) 43
Joint Money Laundering Steering Group (JMLSG), UK 80, 91
judicial systems 60
jurisdictions tool 144, 145

Know Your Customer (KYC) 2, 55, 75, 79, 80, 83, 94, 113, 125
Ku Klux Klan (KKK) 305

Lafarge case 20
law enforcement agencies 52, 60
    see also Federal Bureau of Investigation (FBI); police forces
laws, conflicts of 301
lawsuits 207
layering 5, 7–8, 17, 131, 236
legal framework
    international 26–36
    national 58–9
    and privacy rights 39
    US/UK xi, 36–8
letters of credit/documentary credit 130–1
Liberation Tigers of Tamil Eelam (LTTE or Tamil Tigers) 18, 19, 304
Liberty Reserve case 16–17, 290
licensing/registration system
    currency exchange offices 30
    money value transfer services 50
line management 64
Lloyds TSB 195–6
loan accounts 7
lower-risk customers 83, 134

machine learning xiv, 103, 104
Madeline Investments SA 197
Magnitsky Case 10–11
Malta 44
    Financial Assets Act (VFA) 44
mandate, breach of 302
mandatory reporting 79, 100, 102
Massieu, Luis 199
material deficiency findings 75, 79
Middle East and North Africa Financial Action Task Force (MENAFATF) 53
Milgram, Stanley 65–6
mirror trading 190
Misan, Albert 197
mitigating factors, and integrity risks 212–13
Moldindconbank 9
Monero 8, 17
money laundering 6–18
    criminalisation of 47
    crypto-laundering and Blockchain 12–18
    defined 2
    key processes in 5, 6–8
        integration of laundered assets 5, 12, 236
        layering 5, 7–8, 17, 131, 236
        placement 5, 6–7
    non-cash 9–10
    risk 2
    and terrorist financing, differences between 5, 6, 21–2
    transportation and consolidation 6
    typologies 231–2, 233–56
        alternative remittance services 233–5
        auctions 236–8

black market peso exchange 238–40
'blood' diamonds 240–2
casinos 242–4
correspondent banking 244–6
credit cards 247–9
insurance policies 249–52
mortgages 252–3
trade finance xiii, 254–6
money service businesses (MSBs) 169, 174, 179, 288
MONEYVAL 53, 309
money value transfer services (MVTS) 50
monitoring of accounts *see* transaction surveillance/monitoring
Montero, Edward 197
mortgages 252–3
'mule accounts' 19
Multilateral Development Banks (MDBs) 207–14
Multilateral Trading Facility (MTF) 35
mutual legal assistance 307–8

name check portals/filter systems 98–9
name matches 88, 113
name screening 56, 65, 78–9, 86–9, 100
action when information is inconclusive 88
compliance 89
false positives 89
initial and subsequent screening 87–8
name match vs target match 88
pre-lists 87
private banking 94
sanctions lists 87, 88
national AML/CFT framework, key components of 58–60

National Commission on the Terrorist Attacks upon the United States 4
Nation of Islam 305
neo-Nazis 305
Netherlands Public Prosecution Service (NPPS) 193, 194
'new' terrorism 304–5
New Zealand 37
9/11 terror attacks 4, 249, 261
nominees 37
non-cash laundering 9–10
Non-Cooperative Countries and Territories (NCCT) List 46, 208–9
non-profit organisations (NPOs) 5, 48, 96–8, 144, 263–4
    see also charities; humanitarian organisations
normal due diligence (NDD) 137, 151–3, 162–3
    financial institutions 169, 172
    private banking 180–1
    retail/consumer banking business 175–6, 177
nuclear weapons 42–4
numbered accounts 179

Office of the Comptroller of Currency (OCC), US 85, 192, 206
Office of Foreign Assets Control (OFAC), US 87, 98, 210
offshore accounts 37
Offshore Financial Centres (OFC) 210
offshore trusts 159
'old' terrorism 304
OneCoin 291
online auctions 236
online banking 90–1
organisation structure, AML/CFT role within 63–4
organised crime 210
    see also transnational organised crime (TNOC)

Organization for Economic Co-operation and Development (OECD) xi, 40, 41
Global Forum on Transparency and Exchange of Information for Tax Purposes 40, 210
Organized Crime and Corruption Reporting Project (OCCRP) 8
originator information 82, 92, 246, 262
overseas money transfers 7, 8, 261–2

Palermo Convention (2000) 306–8
Palestinian Islamic Jihad 33
Panama Papers 32
Patriot Act (2001), US 36, 122
payable through accounts 50
penal systems 60
Perepilichnaya, Alexander 10
performance management 71
periodic review process 134–5
personal current accounts 130
personal information 138–9
of corporate nature 139
Pfeiffer, Stephen 205
Pinochet, Augusto 204–6
placement 5, 6–7
PNC Financial Services Group Inc. 206
pocket banks 245, 320
police forces 60, 309
policies and procedures 62, 69, 75–6, 78–9, 86
politically exposed persons (PEP) 2, 30, 32, 50, 55, 88, 95, 99, 314–15, 316, 317, 318–19
and customer acceptance procedures 80–1
enhanced due diligence (EDD) 30, 31, 157, 174, 211–12
FATF defintion of 127
private banking 92, 94

and risk-based approach 127–8
politics
as barrier to international cooperation 301
and terrorist financing 21
Ponzi schemes 291
predicate offences 47, 48
pre-lists 87
privacy rights 39, 47
private banking 92–4
client identification and due diligence 93
counter-terrorist financing principles 94
customer due diligence (CDD) 93, 178–83
enhanced due diligence for higher risk accounts 36, 93–4
name screening 94
politically exposed persons (PEP) 92, 94
pro-business approach 114–15
product risk assessment 129–33
corporate treasury foreign exchange services 131–2
credit cards 131
hedge funds 132
letters of credit/documentary credit 130–1
personal current accounts 130
personal household insurance 133
product type and distribution channel 123–4, 126, 175
prohibited relationships *see* unacceptable clients/relationships
proliferation financing 42–4, 48
prosecutory authorities 60
public disinformation 319
publicly quoted companies 159

Rabobank 192–3
ransomeware attacks 290

real estate 7, 32, 144, 253
record-keeping 50, 57, 79, 83
    minimum periods 83
    type of information retained 84
Reed, John 203
regional bodies 45, 46, 53–4
regulations/regulatory bodies 126
    national 59
relationship risk 133–7
religious organisations 5, 144, 259–61
reporting obligations 84–6
    see also suspicious transaction reports
reputational risk 2, 185–228
    defined 186
    managing 186–7, 207–14
    Multilateral Development Banks (MDBs) 207–14
    when banks go wrong: cases of punishments and penalties 187–206
retail/consumer banking business, customer due diligence (CDD) 174–178
Riggs Bank 204–206
risk-based approach 30, 31, 47, 56, 81, 83, 102, 119–83, 213
    background to 120–2
    components of 122–4
    construction of 128–38
    customer due diligence *see* customer due diligence
    mitigating controls 124–6
    politically exposed persons (PEPs) 127–8
    and regulatory environment 126–7
    relationship risk 133–7
    to training 107, 125–6
risk indicators 122–4

rogue states 26, 28
Rohn, Carlos Hank 3, 196, 197, 198
Rukavina, Hubertus 197, 201
Russia 10, 43, 46, 85
    cryptocurrency regulation 45
Russian Laundromat 8–9, 294

safe deposit boxes 32
'safe harbour' laws, US 86
Salinas, Raul 2–3, 196–204
sanctions regimes 42–3, 48, 65, 87, 169, 179
screening
    staff and third-party 79
    see also name screening
secrecy, culture of 166
'secrecy' products 92
Securities and Exchange Commission 210
self-certification 108
senior management
    approval of high-risk business 81, 90, 124
    hostility to AML issues 166
    over-ruling of compliance 166
    responsibilities 321–3
    support from 65, 69–70
Sergei Magnitsky Act, US 10
shell banks 8, 36, 50, 57, 90, 168, 179, 195, 245, 246
shell companies 8, 9, 37, 294, 320
Silk Road case xi, 15–16, 290
simplified due diligence (SDD) 30, 31–2, 57, 137, 151, 159, 165
    financial institutions 170, 173
slavery, modern-day 284–9
'smell test' 318

Smoke and Mirrors case study 312–23
'smurfs/smurfing' 6, 85, 243
social media 293
South Africa 37
sovereignty 301
speciality, principle of 307
staff education and training 57–8, 75, 77, 86
    certification 108
    CFT elements 108, 110–14
    e-learning 7, 8, 9
    in recognising money laundering/terrorist financing typologies 232–3
    risk-based approach 107, 125–6
    Training Needs Analysis (TNA) 105–7, 111
    training review 111–12
    wide approach to 107–8
staff screening 79
Standard for Automatic Exchange of Financial Account Information in Tax Matters 41
state complicity 301
state theft 284, 294–7
statistics, maintenance of 53
statutory instruments 59
Strasbourg Convention (1990) 29
'stripping' 196
Sudan 196
suspicion recognition 22–4, 110, 229–97
    account analysis examples 233, 264–79
    'accumulation of evidence' cases 233, 280–4
    areas of rising concern 284–97
    background and general principles 230–3

see also money laundering, typologies; terrorist financing, typologies
suspicion reporting systems 115–17
suspicion spectrum 230
suspicious transaction reports (STRs) 38, 49, 51, 52, 57, 65, 79, 84, 115, 116, 117
suspicious transactions/activities 75
characteristics of 84
Switzerland
cryptocurrency regulation 44
Financial Market Supervisory Authority (FINMA) 44

Taliban 19, 28, 301, 321
Tamil Tigers 18, 19, 304
tax evasion xi, 10, 39–42, 45, 47, 210
telephone banking 90
terrorist financing 18–20
criminalisation of 48
defined 2
and innocent society 22
key processes in 5
and money laundering, differences between 5, 6, 21–2
and politics 21
recruitment operations 292–4
risk 2
and staff training 108, 110–14
typologies 18–19, 110
charitable funds 5, 18, 19, 144, 256–7, 263
international business transactions 258–9
non-profit organisations (NPOs) 5, 144, 263–4
overseas funds transfers 261–2
religious organisations 5, 144, 259–61

third parties 80, 80, 95–6
Thomson Reuters 98
three-line defence model 64, 72, 125
tiered ownership 80
‘tipping-off’ 51, 52
trade-based money laundering xiii, 254–6
training *see* staff education and training
transaction laundering xiii
transactions
    re-characterisation of 166–7
    records 49–50, 57
    types 124, 126
transaction surveillance/monitoring 79, 99–100, 101, 121, 142
    application of AI in 104–5
    frequency and depth of 125, 134–5
transnational organised crime (TNOC) 300, 302–5, 314–15
Transparency International Corruption Perceptions Index 96, 128
transportation 6
Trasta Komercbanka 9
traveller’s cheques 19
trigger event reviews 134, 135
Trocca Ltd 197–8, 201
trusts 37
    offshore 159
‘turf’ considerations 301

UBS 193
UN 45, 98
    blacklisting 28, 210
    sanctions regime 87, 169
UN Convention against Illicit Traffic In Narcotic Drugs and Psychotropic Substances (1988) 26

UN Convention Against Trans-National Organised Crime (2000), (Palermo Convention) 306–8
UN Convention on Psychotropic Substances (1971) 26
UN Convention for the Suppression of the Financing of Terrorism (1999) 26, 28, 112
UN Security Council Resolutions 42, 48
1267 (1999) 28
1373 (2001) 28
1624 (2005) 29
UN Single Convention on Narcotic Drugs (1961) 26
unacceptable clients/relationships 142–3, 168–9, 174, 179
Unexplained Wealth Orders (UWOs) xi, 37–8
United Kingdom (UK) 43, 85
Criminal Finances Act (2017) 37, 38, 41–2
Financial Conduct Authority 186, 190
Joint Money Laundering Steering Group (JMLSG) 80, 91
United States (US) 54, 85, 304, 305
Bank Secrecy Act 37, 204
Central Intelligence Agency (CIA) 128
Comprehensive Iran Sanctions, Accountability and Divestment Act (CISADA) (2010) 42–3, 87
Department of Treasury Anti-Terrorist Financing Guidelines 80, 97–8
Federal Bureau of Investigation (FBI) 210
Federal Reserve 186
Final Rule on Customer Due Diligence xi, 37
Financial Crimes Enforcement Network (FinCEN) 192, 195, 285
Foreign Account Tax Compliance Act (2010) xi, 40–1
Internal Revenue Service (IRS) 40
Iran Transactions Regulations (1996) 43
National Commission on the Terrorist Attacks on 4
and ‘new’ terrorism 304, 305

9/11 terror attacks 4, 249, 261
Office of the Comptroller of Currency (OCC) 85, 192, 206
Office of Foreign Assets Control (OFAC) 87, 98, 210
Patriot Act (2001) 36, 122
'safe harbour' laws 86
sanctions list 87
Securities and Exchange Commission 210
Sergei Magnitsky Act 10
transaction monitoring 99
unusual/purposeless transaction 95
US Bancorp 191
US Bank National Association 191

verification 140–1, 151, 159–60, 316
Vienna Convention (1988) 26
virtual currencies *see* cryptocurrencies

Wannacry attack (2017) 290
'war on drugs' 26
wealth, source of 146, 148–9, 212
weapons of mass destruction (WMD) 42–4, 45, 48, 305
Western Express International case 290
wire transfers 19, 50–1, 83, 84, 87,
91–2, 97
withholding tax 40
Wolfsberg Group 55, 80, 90, 93, 94, 122, 170
Wolfsberg Questionnaires 55, 90, 170, 337–55
World Bank 45, 54, 79, 81, 90, 95, 95–6, 294
World Check 98
World Church of Creator 305